DOCUMENT RESUME

ED 444 226 EA 030 518

TITLE	Legal Issues & Education Technology: A School Leader's Guide.
INSTITUTION	National School Boards Association, Alexandria, VA. Council of School Attorneys.
ISBN	ISBN-0-88364-222-0
PUB DATE	1999-00-00
NOTE	99p.; A Technology Leadership Network Special Report.
AVAILABLE FROM	NSBA Distribution Center, P.O. Box 161, Annapolis Jct., MD 20701-0161 (Stock Number 03-145-44, $35 plus $7 shipping and handling). Tel: 800-706-6722 (toll-free); Fax: 301-604-0158; Web site: http://www.nsba.org/itte/publicat.html.
PUB TYPE	Guides - Non-Classroom (055)
EDRS PRICE	MF01/PC04 Plus Postage.
DESCRIPTORS	*Computer Mediated Communication; *Distance Education; *Educational Technology; Electronic Mail; Elementary Secondary Education; *Internet; Leadership; *Legal Responsibility; *Privacy; Public Schools; School Safety
IDENTIFIERS	National School Boards Association

ABSTRACT

Rapid development of new technologies has outpaced the development of related law, leaving educators in doubt about the management of copyright, privacy, liability, and security. A key provision of facilitating a healthy and safe environment for technology use is the school district's "Acceptable Use Policy" (AUP), which states that use of district technology is a privilege, not a right, creating a framework for use and penalties for infractions. Web sites offering sample AUPs are listed in this guide. Chapter 1 introduces AUPs and ways to address issues of freedom of expression, privacy, online pornography, censorship, filtering, and equitable access to technology. Chapter 2 looks at the many administrative issues involved in integrating technology in schools that affect students, faculty, and staff. Chapter 3 recommends developing an AUP expressly for employees to set the stage for a smooth-running network. Chapter 4 examines how new laws are developing to address the rights of creators, the public, and schools related to digital works. An appendix describes legal developments surrounding pornography, a glossary of technology terms spells out some of the acronyms and "computerese," and lists of books from NSBA's Technology Leadership Network and Council of School Attorneys lead to further assistance. (DFR)

Reproductions supplied by EDRS are the best that can be made
from the original document.

ED 444 226

LEGAL ISSUES & EDUCATION TECHNOLOGY

A SCHOOL LEADER'S GUIDE

PERMISSION TO REPRODUCE AND DISSEMINATE THIS MATERIAL HAS BEEN GRANTED BY

J. Floyd

TO THE EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)

1

U.S. DEPARTMENT OF EDUCATION
Office of Educational Research and Improvement
EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)

☐ This document has been reproduced as received from the person or organization originating it.

☐ Minor changes have been made to improve reproduction quality.

• Points of view or opinions stated in this document do not necessarily represent official OERI position or policy.

A PUBLICATION OF THE NATIONAL SCHOOL BOARDS ASSOCIATION'S
COUNCIL OF SCHOOL ATTORNEYS AND TECHNOLOGY LEADERSHIP NETWORK

EA 030 518

BEST COPY AVAILABLE

Legal Issues & Education Technology

A School Leader's Guide

Copyright © 1999, National School Boards Association. All Rights Reserved.

ISBN 0-88364-222-0

A Technology Leadership Network Special Report developed by the National School Boards Association's Council of School Attorneys and ITTE: Education Technology Programs

Authors/Editors

Edwin C. Darden
Staff Attorney
NSBA Office of General Counsel
Alexandria, Virginia
edarden@nsba.org

Rodney A. Satterwhite
Partner
McGuire Woods Battle & Boothe
Richmond, Virginia
rasatter@mwbb.com

Calvin S. Spencer, Jr.
Associate
McGuire Woods Battle & Boothe
Charlottesville, Virginia
csspence@mwbb.com

Ronald D. Wenkart
General Counsel
Orange County, California
Department of Education
Costa Mesa, California
Ron_Wenkart@ocde.k12.ca.us

Margaret-Ann F. Howie
Legal Counsel to the Superintendent
Baltimore County, Maryland, Public Schools
Towson, Maryland
mhowie@bcps.net

Bruce W. Smith
Partner
Drummond Woodsum & MacMahon
Portland, Maine
BWS@dwmlaw.com

Anne W. Ward
Publications Manager
NSBA ITTE: Education Technology Programs
Alexandria, Virginia
award@nsba.org

R. Craig Wood
Partner
McGuire Woods Battle & Boothe
Charlottesville, Virginia
rcwood@mwbb.com

Reviewers/Contributors

Donald Austin
Legal Counsel
Ventura Unified School District, California

Randall G. Bennett
Assistant Director of Risk Management
Tennessee School Boards Association

Janis Bruwelheide
Professor, Project Director, US West Montana Teacher Network
College of Education, Health, & Human Development
Montana State University

Nick Caruso
Senior Staff Associate for Communications
Connecticut Association of Boards of Education

Michael L. Dodd, Esq.
Ferrara, Fiorenza, Larrison, Barrett & Reitz, P.C.
East Syracuse, New York

Greg Ellis
Senior Attorney
Texas Association of School Boards

Eugene School District 4J, Oregon

Michael Gilbert
Technology Director
Massachusetts Association of School Committees

James Hirsch
Director, Instructional Technology
Plano Independent School District
Plano, Texas

Keith Mann
Director, Media Services & Technology
Township High School District #214
Arlington Heights, Illinois

Plano Independent School District, Texas

Scott Price, Esq.
General Counsel/Technology Coordinator
South Carolina School Boards Association

Henry F. Sobota, Esq.
Ferrara, Fiorenza, Larrison, Barrett & Reitz, P.C.
East Syracuse, New York

August W. Steinhilber, Esq.
Reese & Carney, LLP
Annapolis, Maryland

Texas Association of School Boards

James D. Troxell, Esq.
Squire, Sanders & Dempsey L.L.P.
Cleveland, Ohio

... and many others

Excellence and Equity in Public Education through School Board Leadership

Dear Education Leader:

Students and teachers are increasingly finding new ways to enhance the learning environment by relying on technology to open an electronic window to information, images and interactive exchanges around the globe. The Internet, for instance, has been called "the world's largest library."

Legal concerns are a pragmatic partner in this exciting march toward harnessing such wonderful potential. In this context, the law assigns responsibilities and liabilities and prompts thoughts about concepts such as privacy, copyright and keeping students of all ages safe from inappropriate material.

Legal Issues & Education Technology: A School Leader's Guide assists educators in exploring the important issues that arise when law and technology intersect. No school should be without an Acceptable Use Policy – but the parameters and details vary based on the size of the district, the sophistication of the technology itself, the students and/or staff to which the policy applies and other circumstances.

This book is prompted by a clamoring from educators for information about the law and its affect on school technology. Hearing the need, the National School Boards Association leveraged the expertise of its Council of School Attorneys and its Technology Leadership Network to raise issues for discussion and furnish practical advice based on current knowledge. Much of the legal terrain remains unknown and untested, and what we do know for certain is not widely disseminated. This book fills the need and provides answers to some of the most vexing questions that lurk in the background and deserve a more deliberate and reflective treatment.

We wish you success in implementing a technology approach that permits students liberation for learning while ensuring that the school district's policy is legally sound.

Barbara M. Wheeler
President, NSBA

Anne L. Bryant
Executive Director, NSBA

Ann L. Majestic
Chairman, NSBA Council of School Attorneys

BEST COPY AVAILABLE

National School Boards Association
1680 Duke Street ▪ Alexandria, Virginia 22314-3493 ▪ (703) 838-NSBA ▪ FAX: (703) 683-7590 ▪ http://www.nsba.org

Table of Contents

Introduction i

Chapter 1 **School District Policies for Student Use of the Internet & Electronic Publication of Student Works** 1

Resources 21

Sample Documents 23

Chapter 2 **Administrative Issues in School Technology** 25

Resources 41

Chapter 3 **Legal Considerations in Regulating Employee Use of School Technology** 43

Employee Acceptable Use Policy Considerations 49

Health Risks Associated with Technology Use 53

Chapter 4 **Copyright in the School Domain** 55

Resources 72

Sample Copyright Permission Request 74

Appendix **Pornography, the Communications Decency Act and the *Reno* Decision** 75

Glossary of Technology Terms 78

Publications of the National School Boards Association's Council of School Attorneys 81

Publications of the National School Boards Association's ITTE: Education Technology Programs and Its Technology Leadership Network 85

Introduction

The development of powerful and versatile technologies such as the Internet, e-mail and CD-ROM unquestionably marks a revolution in learning. Access to resources has been vastly expanded, creating astounding potential for student achievement, personal development, new discoveries, new global understanding and expanded freedom in learning and teaching.

Making those technologies available to students, teachers and staff in schools requires careful planning, adequate funding, strong professional development programs and school buildings equipped with appropriate infrastructure. It also takes education leaders willing and able to accept the challenge of steering their schools and communities in new, often uncharted directions.

Rapid development of new technologies has outpaced the development of related law, leaving educators in doubt as to how to manage issues of copyright, privacy, liability and security. Particularly in the areas of copyright and online communications, thorny new legal issues require special care as school leaders feel their way into the future.

"The key challenge for schools is to balance the hazards against the potential good that can be accomplished by allowing access to the tools of e-mail and the Internet," says Ronald Wenkart, general counsel for the Orange County Department of Education in Costa Mesa, California, and co-author of Chapter 1. Local school districts must choose the best approach for their schools and communities.

A key provision of creating a healthy and safe environment for technology use is the school district Acceptable Use Policy, stating that use of district technology is a privilege, not a right, and creating a framework for use and penalties for infractions. Some school districts create separate AUPs for students and faculty/staff; others select a single policy for all to live by. You will find Web sites offering sample AUPs on page 21.

Legal Issues & Education Technology: A School Leader's Guide has been created by the members and staffs of two groups within the National School Boards Association: the Council of School Attorneys, composed of 3,000 education-focused attorneys, and the Technology Leadership Network, a group of 460 school districts dedicated to creating positive school change with the help of technology. Both organizations are founded on individuals' desire to create optimum learning environments. In this new book, they join together where their special interests meet.

Chapter 1, "School District Policies for Student Use of the Internet & Electronic Publication of Student Works," introduces Acceptable Use Policies (AUPs) and ways to address issues of freedom of expression, privacy, online pornography, censorship, filtering and equitable access to technology. Here you will find a list of elements important to include in AUPs.

Chapter 2, "Administrative Issues in School Technology," looks at the many administrative issues involved in integrating technology in schools that affect students, faculty and staff. Guidance steers the handling of sexual harrassment and discrimination claims; using e-mail in litigation; limiting e-mail among board members in light of state "sunshine laws;" coping with the Year 2000 problem; making school Web sites comply with the Americans with Disabilities Act; and securing technological equipment.

Chapter 3, "Legal Considerations in Regulating Employee Use of School Technology," recommends developing an AUP expressly for employees to set the stage for a smooth-running network. Privacy rights, First Amendment issues, collective bargaining matters and safe computer-use practices are discussed.

Chapter 4, "Copyright in the School Domain" examines how new laws are developing to address the rights of creators, the public and schools related to digital works. Discussions of the Copyright Act (1976); its amendments, the Digital Copyright Millenium Act (1998) and the Copyright Term Extension Act (1998); and the important doctrine of "fair use" in education will help you address copyright issues.

An appendix describes legal developments surrounding pornography; a Glossary of Technology Terms spells out some of the acronyms and "computerese;" and lists of books from NSBA's Technology Leadership Network and Council of School Attorneys lead you to further assistance.

Armed with an understanding of the issues, relevant law and where to find more information, you and your colleagues will be better prepared to take on the challenges and reap the rewards of integrating technology in your schools.

Chapter 1

School District Policies for Student Use of the Internet & Electronic Publication of Student Works

Ronald D. Wenkart*
General Counsel, Orange County, California Department of Education
and
Edwin C. Darden
Staff Attorney, National School Boards Association

Introduction

Public school access to the Internet raises exciting possibilities for students to engage in self-directed learning, but it also introduces a number of complex legal issues. The student's right to privacy and free speech, for example, must be weighed against the interests of parents and the school district. The object is to prevent access to potentially harmful material, such as pornography. The use of e-mail by students can also raise liability issues due to harassment or defamation.

While instant electronic access to information and live two-way communication offers a world of potential to educators, the Internet poses equally obvious risks and raises myriad concerns for school decision makers. From a legal standpoint, the key to wisely harnessing the Internet's power begins with a clear and detailed "Acceptable Use Policy." Such a policy, distributed and made available widely to parents, teachers, staff, the community and, via the Internet, to the world, can act as both a billboard and a shield.

A sound policy will put parents and students on notice of the rules for acceptable use of school technology and diminish parents' and students' expectation of privacy. A sound policy will establish parameters for acceptable student behavior while using school technology and will allow the school district to review all e-mail. A strong policy must allow school officials to discipline those who violate the terms of the policy. It must also specify that school personnel will, to the extent possible, supervise technology access.

The Internet is a network that enables students to access huge compendiums of information via personal computers at school, usually located in classrooms and media centers.

Establishing Web sites – or places where anyone with a computer and modem can tap into and receive images, sound and text – is popular among schools. Web66 (a site operated by the University of Minnesota College of Education, *http://Web66.coled.umn.edu/schools.html*) maintains an International Registry of Schools on the Web. According to its most recent statistics, more than 13,400 schools were registered with Web 66 as being on the Internet as of July 1998 – approximately 8,840 school buildings in the United States.

* *A biographical sketch of the authors is available at the end of this chapter.*

A survey of 1,000 schools by the U.S. Education Department's National Center for Education Statistics found that school Internet access nearly doubled in 1998. More than 50 percent of classrooms, school libraries, media centers and computer labs had Internet access, up from 27 percent when the same survey was taken in 1997. The survey also determined that the northeast lagged behind in the volume of Internet connections. Also, schools with Internet access are deploying the latest technology, with most — 65 percent — using a high-speed connection rather than dial-up access.[1]

The first part of this chapter is devoted to the all-important Student Acceptable Use Policy. Without endorsing any one approach, it will discuss the elements that are important to consider and will explain how a good policy can be the saving grace when a lawsuit hits. The second part will explore the legal issues that arise from student use of the Internet. For example, should students publish creative works on the district Web site? What liability arises from student access to e-mail? And how do schools prevent students from viewing inappropriate information in cyberspace?

Acceptable Use Policy

The natural starting point for developing a comprehensive and coherent approach to student Internet and technology access is the Acceptable Use Policy (AUP). A well-designed AUP lays the foundation and sets forth conditions under which students are allowed to use the Internet and other school technologies.

This approach in essence becomes the contract between the school, the student and the parent or guardian. Legally, it sets forth expectations and puts everyone on notice as to "acceptable use," and it helps protect the school against later claims. While it is best to address specific topics, school officials and attorneys may want to consider leaving the language flexible enough to cover unforeseen or currently unknown possibilities that arise in the course of student conduct. Preferably, the AUP is primarily a specific document, addressing such matters as the right of school districts to review browser logs (which track what sites students have viewed). The AUP outlines discipline procedures for violations, requires adult permission for technology use and details other central tenets of the school district's position relative to technology.

One common mistake is trying to be as broad as possible, resulting in language that is vague and may not survive federal court scrutiny. Students within a school setting still have constitutional free speech rights, and an Acceptable Use Policy that constricts that right unnecessarily may be subject to a First Amendment challenge. Statements like "students shall not have access to unacceptable or offensive material" may sound good in the abstract, but a court may view it as vague and without real meaning. If so, the court might declare it unconstitutional because readers and users were not placed on fair notice of what was permissible and what was not. Furthermore, the court may say such language is overbroad, sweeping into its scope a number of topics that ought to be protected by free speech principles.

School districts must be unequivocally clear that access to the "international network of interconnected computers" – commonly known as the Internet – is a privilege and not a right. Permission to use school technology, therefore, will be withdrawn if there is a violation of rules, policies or generally accepted conventions.

Another consideration for a prudent school district is whether the Acceptable Use Policy or the general discipline policy will seek to punish students for off-campus behavior that has the potential of causing on-campus disturbances. For example, what can a school district do with a student who creates a "hate site" featuring a loathed teacher at school, a nemesis classmate or the guy who refused to ask her out for a date? Also, what if the student site includes sexually explicit matter and is linked back to the official school site?

1. *See* "Internet Access in Public Schools and Classrooms: 1994-1998" at *http://nces.ed.gov*.

FREE EXPRESSION

Can racist political speech be linked to the school's Web site?

Local racist John Doe is running for the school board. He places information on the school district Web site and proceeds to engage in a political debate about the school board election, decry the shameful information being taught in the district's schools, and make scurrilous remarks about the abilities of various school employees.

Now what?

Can religious groups have their link?

The Generica High School Rally 'Round the Flag Pole Club (Christian prayer group) begins posting material on the school Web site. It turns out to be one of the most visited connections to the Web site — not because of its religious content, but because of its "Sinner of the Week" column. Club members vote on which teacher or student was the biggest sinner during the previous week, write about which Commandment was broken, and give details on the actions that the sinner took in breaking the Commandment.

Any problem with the district prohibiting this practice?

Answer: If the Web site is an open forum for expression, it's the cyber-age equivalent of a soap box in a park. Therefore, everyone is entitled to a say. Since schools must be neutral toward religion, they may not restrict their own prayer club from posting information on the Web site. (*See Board of Westside Community Schools v. Mergens*, 109 S.Ct. 3240 (1990)). The school district can, however, declare the site a closed forum and squelch all voices but its own.

In Missouri in late 1998, a federal district court found in favor of a student, granting him a preliminary injunction in response to the district's 10-day suspension. The student had created a Web site at home that said critical things about the school district and some of the people at school. He then linked his page to the official district home page. Fearing disruption, school officials called on him to halt the practice. The case could go to trial some time in 1999.

Schools should know that the ability to control off-campus student behavior in relation to Web sites that bear a school connection is unknown legal terrain. Courts will have to carefully balance the free speech rights of the student versus the need of school officials to maintain a safe, orderly environment free of hostility engendered by electronic sniping.

This problem is likely to get worse as students learn, as part of their general education at school, how to create and manipulate Web sites. Through techno-literacy students will also grow more clever in their ability to engage in electronic rebellions.

In a tribute to the importance of Acceptable Use Policies, the state of Indiana took the step of writing the need for AUPs into law. In September 1995, the Indiana Department of Education required schools in the state providing Internet access to K-12 students to adopt state *Guidelines for Acceptable Internet Use* in order to receive financial assistance for their Internet access.

Finally, school districts face the question of whether to have a single policy that covers both students and school district employees or to create a separate policy. This is largely a philosophical and practical issue that deciding officials should discuss

with their attorneys. Each approach has its advantages and disadvantages. For example, a single policy allows there to be a singular standard for everyone and avoids confusion about which rules apply to which populations. A separate policy, however, allows a district to tailor the policy to the specific needs and circumstances unique to students on one hand and workers on the other. [For a point of view that advocates a separate employee policy see Chapter 3: *Legal Considerations in Regulating Employee Use of School Technology*.]

FREE EXPRESSION

Can a student create a private Web site disparaging school & teachers?

A group of enterprising students at Fallacy High School create their own Web site without using any school district technology. The Web server for their site is a private Web server. They call their Web site the "Fallacy High Hi-Times." On their Web site, students post articles favoring the legalization of illicit drugs, and euthanasia of teachers over the age of 30. And they write disparaging articles about Fallacy High School, the Fallacy administration, the Fallacy faculty and student leaders at school. People logging onto the Web site could believe it is a Fallacy High School sponsored Web site.

Does the school have any leverage in preventing publication of this Web site and material?

Answer: These are untested principles in an emerging area of the law. It is an open question as to whether school districts have the right to discipline students who do not use school-owned technology and yet engage in speech that is potentially disruptive to the school community. Incidents of this type that have flared up in various parts of the country have been met with mixed success by school districts and mixed answers by the courts.

Publishing student work on the school district Web site

One of the most difficult issues that schools are struggling with is how to deal with displaying student work on Web sites. While students, faculty and parents are rightfully proud of achievements produced in school, the idea of placing artwork, writing or other student creations on a universally accessible electronic site is problematic unless school districts implement some basic precautions.

The starting point is asking the question: should student work ever be displayed on a school district's Web site? The difficult part of that assessment is achieving the delicate balance of wide dissemination while protecting privacy and ensuring the safety of students, regardless of their age.

Advantages of Internet Web site displays are obvious – they enable instant access at any time by a remote user. Thus, despite distance, the relatives, friends and mentors of a student can see concrete evidence of their favorite pupil's growing prowess. Further, the school or district Web site provides one more medium for publication – giving students another goal to strive for and another plaudit to include on resumes or in a biography of accomplishments. Some aspiring high school students, for instance, want their work displayed electronically because they can easily refer colleges to the site to see a portfolio of their abilities.

The disadvantages are equally apparent. Individuals with bad intentions can use information they obtain – names, interests, location – to bring harm to a vulnerable population. Liability in instances where someone uses a school-sponsored Web site as a source of information is probably remote, but schools could potentially be held responsible.

Therefore, schools districts should seek to gain all the positive attributes of Web publishing while minimizing the risks. One way to accomplish this is to create a Web publishing policy that

requires explicit parental permission – through a *signed release – that authorizes the school district* to display the student's work on its Web site. This should be a stand-alone release, not to be confused with the more common release that allows photographs of students to be taken and "published." In addition, districts must decide if a one-time release will suffice, or if it will seek permission each time a separate work is considered for the site.

While the Web has been compared to a newspaper, it is not at all clear from a legal standpoint that the two are precisely equivalent. A paper document could be disseminated worldwide, but it would take a more intentional act and perhaps more effort on the part of the information seeker to obtain it. The electronic age enables a computer user anywhere in the world to access information by and about students with just a "click" of a computer mouse.

In Eugene, Oregon, for example, the school district's policy requires that only the first names of students can be published, that pictures of *students not be accompanied by identifying* information and that a student's home address and telephone number never may be included. In addition to protecting students, this policy could help school officials and teachers involved in a court proceeding to make the case that the district acted reasonably considering both the circumstances and the risk.

Schools should be especially careful about allowing school personnel to create class-specific Web sites, school-specific sites or other stand-alone presentations. A legally sound policy should either (1) forbid the practice, instead requiring all submissions to be located on the district-wide or building-wide Web site, or (2) establish a rigorous pre-clearance requirement that allows a responsible official to screen and approve possible submissions.

Links to a school Web site or a district Web site supply another source of potential liability. For example, a parent and/or student could sue the

SAMPLE WEB PUBLISHING STATEMENT

Preamble

It is clear that there are significant risks, as well as significant advantages, involved with allowing students to be identified on the Internet. Therefore, students should not be easily identifiable from materials they might publish on the Internet. No directory information should be posted on the Web for students whose parents have returned the form asking that such information not be released.

Guidelines:

- Preferably, only the student's first name will be used in published student work.
- Pictures that are a part of student publishing should not include identifying information.
- Under no circumstances should a student's home address or phone number be included.
- If replies to published student work are appropriate, the sponsoring teacher's address should be the e-mail address displayed, not the student's.
- In special circumstances with parent-signed release, identifying information can be added.

— Lane County School District No. 4J, Eugene, Oregon, *4J Student Internet Privacy Guidelines*

school system for injuries caused by information received from a Web page linked to a school-sponsored Web page. While the risk of losing a case of this type is slight; it could certainly cause an embarrassment for the district. It would be difficult for a plaintiff to meet the burden of proof necessary to hold the school district responsible for whatever harm befell him or her.

For example, a school-sponsored Web site might link to an unrelated site that contained its own link to a separate site advocating racial bigotry. It would be difficult for the plaintiff to convince a judge that the school district was embracing or promoting such ideas. Moreover, there is a provision in the Communications Decency Act[2] that appears to be a "safe harbor" against such lawsuits for Internet service providers, which includes school districts. To avoid problems, however, school districts should scrupulously research all proposed links it places on the school-sponsored Web site to make sure the connection is free from objectionable material. Perhaps a disclaimer posted at the school district's Web site might read:

> ***Links to Third Parties' Sites***
>
> *The links in this area will let you leave the school district site. The linked sites are not under the control of the district, and the district is not responsible for the contents of any linked site or any link contained in a linked site, or any changes or updates to such sites. The district is providing these links to you only as a convenience, and the inclusion of any link does not imply endorsement of the site by the district.*

Additionally, a school district could be sued on constitutional grounds for either allowing or prohibiting the placement of a link on a school-sponsored Web site to another Web site. For example, if a student – under the auspices of school work or extracurricular activity – wanted to create a link from a school district Web site to a Web site containing material promoting religious indoctrination, the district could face either: (1) a lawsuit claiming violation of the separation of church and state doctrine under the U.S. Constitution if the district allowed the link; or (2) a lawsuit from the student alleging a violation of his or her freedom of religion and freedom of speech if the district refused to permit the link.

Since these are new frontier issues, there is no case law available on the subject. But it seems likely that courts would treat a district-sponsored Web site in much the same way it would treat a school newspaper, theatrical production or other expressive activity that one might reasonably perceive as sanctioned by the school and school district.

The U.S. Supreme Court has held in *Hazelwood School District v. Kuhlmeier*, 484 U.S. 260, 273 (1998) that "educators do not offend the First Amendment by exercising editorial control over the style and content of student speech in school-sponsored expressive activities, so long as their actions are reasonably related to "legitimate pedagogical concerns." In other words, a school may prohibit expressive activity that is, for example, ungrammatical, poorly written, inadequately researched, biased or prejudiced, vulgar or profane, or unsuitable for immature audiences.[3]

Perhaps the best way to assure courts treat Web sites equal with other school-sponsored publications is to include the subject within the Student Acceptable Use Policy. For example:

> ***Web Pages***
>
> *All Web pages created by students and student organizations on the district's computer system will be subject to treatment as district-sponsored publications.*

2. The U.S. Supreme Court struck down the criminal penalties section (47 U.S.C. §223[a][1][B][ii]) of the Communications Decency Act in *Reno v. American Civil Liberties Union*, 117 S.Ct. 2329 (1997). However, the "safe harbor" provision (47 U.S.C. §230[c][1]) for Internet service providers (including school districts) remains in effect.

3. See *Kuhlmeier*, 484 U.S. at 271.

FREE EXPRESSION

Who governs electronic newspapers on the school district's Web site?

Nostalgia High has an open guest book for people to share what they think of school programs and the Web site. The school district invites community participation at the Web site with chat rooms, the guest book, and bulletin boards. The school board has proclaimed that it wants the school district's Web site to be as open for expression as a school board meeting. School board members welcome input on the Web site regarding curriculum, important political issues regarding education, and anything that the community considers important in relation to education.

Sophomore Judy Java prints an underground newspaper and distributes it at school. She enjoys criticizing various things about the school, using four letter words and publishing questionable stories and poetry that include vulgar language. Since Judy produces the paper at home, she might actually have a legal right to engage in such activity on campus.

No one pays attention to Judy anymore. She therefore posts her newsletter on the district Web site bulletin board. To make sure people pay attention, she now writes shameful articles about which teachers are drunks and have Driving Under the Influence (DUI) charges now or in the past. She makes allegations about which teachers cheat on their spouses, with whom and when, and about which teachers have made inappropriate advances to students. Judy's articles are widely read and have popularized the district Web site considerably. Judy is even dreaming of a career with one of the Hollywood gossip tabloids.

May the district keep Judy off its Web site?

Answer: Under First Amendment freedom of expression law, when a school opens a forum (like the Web site in this scenario) to unrestricted public expression, it has difficulty thereafter controlling the content and who has access to that forum. Nostalgia High has opened its Web site to the community to discuss its schools. Judy can argue that she is discussing the community schools by revealing which teachers are fit examples for youth. With an open forum Web site, a Court would probably allow Judy to continue her underground link to the school's Web site. (*See Beussink v. Woodland R-IV School District*, 1:98CV93 RWS; U.S. District Court for the Eastern District of Missouri, decided December 28, 1998 (temporary injunction against the school district's 10-day suspension of a student who created a private Web site on the Internet that was critical of the school. The student linked the offending site to the school district's Web site)).

Policy Solution: The school could eliminate expression such as Joe's in two main ways. (1) It could prevent the Web site from being used as a community forum for discussion of education issues; or (2) It could adopt a Web site policy that designates the Web site as a "closed forum" for district use only to transmit information to the public. Note, though, that neither solution would address the unresolved issue of a student creating on a home computer a Web site that includes disparaging comments about the school or its people and that may be linked to the school's official site.

Accordingly, the district reserves the right to exercise editorial control over such publications.

School board members, religious student groups or others with a strong agenda may seek access to the school's Web page. School boards should carefully consider what standards and rules apply in granting access to school building or district Web sites.

In addition to general guidelines, some school districts accomplish the task with academic requirements. They can demand that any student work published on the Web meet standards of spelling, grammar, adequate research or other qualitative measures.

Electronic mail

Many schools allow students to have e-mail[4] addresses. Many schools monitor the e-mail students send and receive.

At the beginning of the school year, or whenever a new e-mail account is established, school districts should obtain written permission from both the student and the student's parent or guardian to monitor electronic mail. The Electronic Communications Privacy Act (ECPA)[5] makes it a criminal offense to intercept e-mail while it is in transit.

The Act provides that it is not unlawful to intercept electronic communication if at least one party to the communication has given his or her consent to the interception. *See Bohach v. City of Reno*[6] which found that the city is permitted to read stored electronic messages without violating ECPA. Even when a student has not returned a consent form, there is some indication that courts will take a lenient view that allows school districts to view students' electronic mail stored on the district's computer. In *Steve Jackson Games, Inc. v. U.S. Secret Service*, 36 F.3d 457 (5th Cir. 1994), the federal court interpreted the Act as not applying to information stored on the provider's system.

Some school districts, operating on attorney advice, decide that in lieu of a student permission slip, they will simply notify parents annually of the risks involved in using education technology. There are several reasons underlying this approach. First, if the school board believes that the Internet is an important educational tool, then all students should have access to it, not just students who have returned consent forms. Relatedly, as the Internet becomes more integral to the curriculum, it will become increasingly difficult for students who do not return the forms to progress with other students. Also, no permission system is failsafe. If a student without a form gains access to inappropriate material, general use of that very

Electronic Communications Privacy Act
The E-Mail Permission Exception
18 U.S.C. §2510-2520

It shall not be unlawful under this chapter for a person not acting under color of law[7] to intercept a wire, oral, or electronic communication where such person is a party to the communication or *where one of the parties to the communication has given prior consent to such interception* unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.

4. E-mail is a customized electronic message that is sent from one computer to another across a network.

5. 18 U.S.C. Sections 2510-2520.

6. 932 F.Supp. 1232 (D. Nev. 1996)

7. This phrase refers to an actual legal right or the appearance of one. It encompasses not only acts done by state officials (including school officials) within the limits of their lawful authority, but also acts done beyond the bounds of lawful authority and made possible only because the wrongdoer is cloaked with the authority of the state.

form could enhance liability accusations.

Perhaps, then, the best approach is to do both. A permission slip is particularly effective when students have an individual account and can get to the Internet via remote access (such as at home or another location). If the only time that a student would have school-related access to the Internet is in the classroom or library and under adult supervision, then perhaps only parental notification is necessary.

Some school districts may encounter special problems if they use an outside network to supply Internet access and e-mail capability. That approach is especially popular in rural school districts and those of limited resources because the cost is low. School districts in that position should consider whether the Internet provider is willing to allow officials access to tracking mechanisms when the need arises, and under what circumstances the two parties might be working at cross purposes. Provisions should be included in the initial contract or as an amendment by mutual consent.

Some school districts decide not to give students e-mail accounts but rather to grant the privilege to teachers and let classroom leaders decide when students need to use electronic means to facilitate learning. Still other districts create "project accounts" that have starting and ending dates and the user name online reflects the project rather than a person. Whatever the technique, the same

HOW TECHNOLOGY CAN AFFECT ETHICAL BEHAVIOR

While many of our traditional values can be stretched to fit the new environment of information technology, some aspects of this new environment can make that fit difficult to perceive. A child who would never think of searching through a classmate's desk to read her personal diary might feel free to access and read the same classmate's diary stored in a word processing file on a computer network. A teenager who would never dream of robbing a bank might experience fewer qualms about attempting to steal funds from the bank electronically. Why?

One explanation is that the technology removes us from the concrete object: the book, the actual money. Another explanation is that, by using the computer to commit an unethical or criminal act, the perpetrator often believes that he or she can escape detection. As the fear of being caught decreases, so does the student's need to engage in soul-searching.

Information technology also introduces psychological distance to the scenario. When we interact with others face-to-face and behave unethically, we experience first-hand the harm we have caused and perhaps ostracism or even quick rebuttal – and the resulting feelings can reinforce our ethical norms. When we use information technology in a way that does harm to others, the act feels less personal because we cannot see or hear the other person in the exchange. For instance, if a group of students gains unauthorized access to a corporate computer network, they might feel pleased that they have succeeded in "beating the system" but might never realize the disruption they have caused to the employees who run and use the network.

Schools play a major role in reinforcing traditional societal values and helping students see how those values apply to the use of information technology. Schools can take action on technology ethics on two fronts: setting school policy that provides a model for students to follow, and incorporating technology ethics issues into the curriculum.

— *Excerpt from* "Ethical Use of Information Technologies in Education: Important Issues for America's Schools," *published in 1992 by the U.S. Department of Justice's National Institute of Justice*

precautions about permission, supervision and acceptable use standards still apply.

In general, e-mail creates its own unique set of issues because of the swiftness of communication. Even with appropriate supervision, a student can quickly create havoc through immature and improper use of the technology. For example, in Marshfield, Massachusetts, several United States Secret Service agents quickly arrived at the school's doorstep with serious looks and multiple questions after a student prankster sent a death threat to President Clinton via the White House Web site. Worse yet, the threat was signed using the name of the school principal.

In February 1999, a high school in Raritan Township, New Jersey, had a similar

LIABILITY

Are schools responsible if a student uses school Internet access to learn how to build bombs — then uses that new-found skill?

Johnny is a very smart and inquisitive seventh grader who has no Internet access at home. His teacher has just taught him how to use the Internet to find information about different subjects, such as the gross national product (GNP) of South American countries and the yearly rainfall in the Congo, both of which are topics Johnny is supposed to be studying in class. Johnny is more interested in other things and spends hours on the Internet learning how to make letter bombs and pipe bombs. No one notices what Johnny is up to until he blows up the local convenience store across the street from the school.

The store owner sues the school and, furthermore, Johnny's parents demand copies of all e-mail Johnny has sent over the school's e-mail system.

Is the school liable? Second, must the school turn over the e-mail?

Answer: If a jury felt that the school district's supervision of Johnny's Internet access was inadequate, the school district might be liable. The Student Acceptable Use Agreement can include "hold harmless" language that seeks to waive liability – so that neither the parent, guardian nor student signing it could sue. Here, however, the store owner is a third party not involved in the agreement. The Student Acceptable Use policy does not extend to that person.

As to the e-mail, in consenting to a Student Acceptable Use Agreement, Johnny and his parent would have waived certain privacy rights, including giving the school permission to monitor his e-mail. In this context, schools might be compelled to relinquish the e-mail during discovery (the question and answer phase of litigation – before trial – when attorneys are compelled to give information to the other side).

Policy Solution: Policies will not prevent liability to third parties such as the convenience store owner. But vigilant supervision of student use of the Internet should, in theory, catch such errant misbehavior. Students browsing bomb-making sites could be subject to school discipline for unauthorized use. Alternatively, schools and teachers can argue to a court that they took reasonable steps to prevent students from acquiring knowledge that could be used to harm people.

experience. A 17-year-old student was charged with harassment after he sent a threatening message to the President. The student, who was in the school's computer lab, was supposed to be working on a science research project.

In another true incident, a student e-mailed a bomb threat to a major national newspaper, costing the threatened organization time, money, and fear while extraordinary precautions were taken. The message was traced back to a school district computer, but the suspected student initially denied any involvement. The computer's log was precise about the time and message. The student's home state and the state in which the newspaper was based both considered filing criminal charges. The student quickly confessed – writing a letter of apology to all whom he had inconvenienced.

The key challenge for schools is to balance the hazards against the potential good that can be accomplished by allowing students access to the tools of e-mail and the Internet. The benefits include having electronic "pen pals," performing research, establishing communications with professionals in key occupations and growing familiar with the "world's largest library," the World Wide Web. Classrooms can connect with others from across the country and around the globe, using Internet technology and school profiles to find just the right match. One of the largest such on-line communities, e-PALS Classroom Exchange (*http://www.epals.com/index.html*) has more than 11,500 classrooms registered, representing 850,000 students in more than 90 countries, and provides information on each class's ages, grade level, language, study projects and other relevant data.

Beyond e-mail, there are the more interactive forms of communication in which students can have items sent to them, can view and participate in bulletin board discussions or can "chat" with other people in real time. Electronic mailing lists Listservs® or e-mail groups organize people who have similar interests and want to share ideas about a particular topic. List members' messages and replies are automatically routed to everyone on the list, allowing all to follow topics of common interest.

Public chat rooms are live electronic conversations that two or more people conduct by typing messages into their computers and transmitting them to a central bulletin board that everyone "in the room" can read. A variation is a private chat, in which two or more people retire to a secluded "electronic space" to chat. The interactive chat feature

Student e-mail should never be considered private

- ✘ E-mail is not a confidential medium for transmitting personal messages.
- ✘ E-mail can be reviewed by others and should be used only for legitimate educational purposes or as authorized.
- ✘ E-mail should be viewed by students as the sending of a written memorandum by electronic means.
- ✘ Students should be informed that their e-mail will be monitored and the discipline policy enforced if infractions occur.
- ✘ There is no guarantee of privacy when using any school technology.
- ✘ Students should be advised not to give personal information over the Internet.

LIABILITY

Are schools responsible when children use school computers for live cyber-chats and become victims of in-person abuse?

Sandra is a 13-year-old middle school pupil who spends hours on the Internet at school. She has no Internet access at home and her parents know very little about the Internet. One of her favorite pastimes is to enter electronic chat rooms and talk to others about personal things like relationships, love, and life experiences. Her teacher lets her use the Internet in the classroom every day at lunch. Sandra meets a wonderful 13-year-old boy via a chat room. He is everything that she dreamed of in a romantic relationship. She arranges to meet him at a local fast food hamburger restaurant. It turns out her chat-room friend is actually a 45-year-old child molester. Sandra is abducted and molested. Sandra and her parents sue the school for negligent supervision.

Could the district and teacher be held liable?

Answer: The school district and the teacher might be held liable if a jury concluded that the teacher's supervision was not reasonable under the circumstances. One way a plaintiff's attorney could prove their case is by calling school administrators from other districts as witnesses to discuss the risks inherent on the Web and the necessity to supervise student use of the Web. This hypothetical is loosely based on a situation that occurred in San Diego. (*Dailey v. Los Angeles Unified School Dist.*, 2 Cal.3d 741, 470 P.2d 360 (1970)) (sets forth duty of student supervision by school personnel.)

Policy Solution: Before allowing students access to the Internet, school districts should require that students and either their parent or guardian sign a Student Acceptable Use Agreement. By including "hold harmless" clauses and a release in that agreement, the district and teacher could argue in some states that they cannot be held legally responsible because such liability was waived. (*Aaris v. Las Virgenes Unified School Dist.*, 64 Cal.App.4th 1112 (Cal. 1998) upholding release language with a school).

Sometimes, school districts choose to forego a permission slip in favor of parental notification that outlines the risks of Internet access. The belief behind that approach is that some students who have not signed a consent form may gain access to the Internet anyway. If that person reads inappropriate material, the consent form then could enhance liability since the school district did not follow its own policy. Perhaps the safest approach is to arrange for both a permission slip and parental notification.

has many educational benefits. In 1997, some students followed a group of space shuttle astronauts as they prepared for their mission, conducting live chats with them to get first-hand information. The down side of chat rooms is that it is difficult to restrict what information students receive or disclose about themselves during the electronic chat session.

Student privacy

Providing Internet access for students raises issues of privacy. Districts should caution students that information is available about their online activities. For example, every time an individual accesses a Web site, the computers and networking equipment involved create a trail that

is stored in a log on the user's computer hard drive. The computer or server that maintains the connection to the Internet also keeps track of which computer has visited which Web sites.

Similarly, some Web sites use "cookies" – a mechanism that instructs the browsing software on the visiting computer to remember the name of the site, passwords and other essential information and store it in a file on the visiting computer's hard disk. Then, the next time the computer pays a visit, the server seeks out the information stored there and reads the information previously collected. These devices are also known as "persistent cookies" or "magic cookies" and can be accessed upon demand – creating yet another tool to determine where students have been with their electronic outreach.

It is imperative that school districts make clear through their policies and communications that the student should have no expectation of privacy in e-mail, Internet use or other work accomplished on school district owned technology. This factor could be the linchpin in defending the right to search for incriminating information when enforcing the Student Acceptable Use Policy. [See Chapter 3: *Legal Considerations in Regulating Employee Use of School Technology* for a further discussion of this topic.]

Family Educational Rights and Privacy Act

The Family Educational Rights and Privacy Act[8] (FERPA) requires districts to have a policy that grants parents the right to inspect and review the education records of their children. FERPA requires that school districts establish procedures to provide parents access to records within 45 days of a request. Educational records are defined as those records, files, documents and other materials that contain information directly related to a student and which are maintained by an education agency or institution. Regulations implementing the Act make clear that this definition for FERPA includes data stored by electronic means.

FERPA also requires that schools obtain a parent's written consent before disclosing personally identifiable information about the student. Most school computers that provide Internet access automatically store information about the student's electronic activities. That data might fall within the definition of education information about students, thus, entitling parents by FERPA to see it. To the extent this information identifies a particular student's use of the school's Internet connection, it could qualify as personally identifiable information that must be protected. If a system is not in place for finding the technology based information efficiently, school officials could find themselves in the midst of a time consuming and challenging task to locate information as the 45-day clock ticks on a request.

Family Educational Rights and Privacy Act (FERPA) – 20 U.S.C. §1232g

- ✘ When exchanging or sharing records with other school districts or public agencies, safeguards must be in place to protect the privacy rights of students under federal law.
- ✘ The same rules of confidentiality apply with respect to student records that are computerized.

In addition, school districts should carefully monitor the type of student information that is provided on school Web sites. As a matter of good practice, generally names and photographs of students should not be placed at a Web site without parental permission.

FERPA is premised on the fact that school districts must comply with its terms to qualify for

8. 20 U.S.C. Section 1232(g)

Should a school district place pictures of students or student work on its Web site?

- ✘ Photographs of students should not be displayed on a school building Web site or district-wide Web site unless prior, explicit permission has been obtained from a parent or guardian.
- ✘ People may view the Internet differently than a standard paper publication. It is more likely that someone outside the school community will intentionally access computerized information – given its easy electronic retrieval – rather than intentionally seek out a paper document. Include a clause in the policy about Internet use and have a separate Internet release in the district's Acceptable Use Policy.
- ✘ Unauthorized use of a student's likeness or other identifiable information could constitute a violation of the Family Educational Rights and Privacy Act (FERPA).

certain federal funds. As a practical matter, a school district would have to be dramatically off base to warrant loss of federal money. But a determined plaintiff could claim under 42 U.S.C. §1983 that the school district violated the student's constitutional rights by the unauthorized release of personal information that should have been protected under FERPA. In that way, school districts could be held liable and forced to pay significant money in compensation. Furthermore, some states have added their own, even stricter, statutes that control access and disclosure of educational records and information. Districts should check to see whether they are located in such a state.

Pornography

U.S. SUPREME COURT DECISION IN *RENO*

In *Reno v. American Civil Liberties Union*,[9] the United States Supreme Court reviewed provisions of the Communications Decency Act, 47 U.S.C. section 223(a)(1)(B)(ii), which imposed criminal penalties for the knowing transmission of obscene or indecent messages to any recipient under 18 years of age. Section 223(d) prohibits knowingly sending or displaying any message that, in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs.

The Court held that the Communications Decency Act (CDA) was overbroad and violated the First Amendment of the U.S. Constitution. The High Court stated that the breadth of the CDA's coverage is unprecedented and that the undefined terms "indecent" and "patently offensive" cover large amounts of non-pornographic material with serious educational or other value. The Court said the CDA's prohibition might extend to discussions about safe sexual practices, artistic images that may include nude subjects, and arguably the card catalog of the Carnegie library.[10]

***U.S. Supreme Court in* Reno**

- ✘ Congress' first attempt to regulate minors' access to pornography on the Internet was struck down as overbroad and a violation of the First Amendment.
- ✘ The Court's decision implied that a more narrowly drawn law would be constitutional.

9. 117 S.Ct 2329 (1997)

10. *Id.*

Developments after *Reno*

- ✘ Since the *Reno* decision, more than 180 bills have been introduced in Congress involving the Internet.
- ✘ The courts have struck down state legislation seeking to regulate the Internet, saying that state statutes are an unconstitutional burden on interstate commerce.
- ✘ A federal district court in California upheld a federal law that prohibits the transmission of child pornography (as defined in existing law) over the Internet.

School officials therefore should be cognizant that the CDA no longer applies but that political concern for an effective method of keeping pornographic material out of the hands of minors still remains. Several proposed laws have been initiated in Congress to put the brakes on what many representatives and senators see as runaway access to unpalatable material.

PORNOGRAPHY

Can students who post pornography to a school's open guest book be punished?

McHay High School students yearly "tip" their opponent's mascot (the roughrider statue) at Yonder High before the big game between the two schools. Since students were caught and punished over the last few years, this year's crop of McHay students has become more creative. They logged onto the opponent's Web site, clicked onto the "Roughrider Guest book," and instead of posting comments about the school and the Web site, they posted several dozen pornographic pictures.

Can they be punished? How can the pictures be removed?

Answers: Given proper due process and a disciplinary policy that is broad enough to include this type of student misbehavior, the students could be punished by their own McHay High School. In addition, the students might face criminal charges if officials were so inclined.

As for removing the pictures, the person controlling the password to the Web server may easily remove the pictures. If the webmaster is off campus (as was the situation in the circumstances this hypothetical is based upon), it could be problematic in immediately removing the pictures.

Policy Solution: Make sure the district's Web site policy creates supervision over district related Web sites by district personnel. It may eliminate chat rooms and guest books to avoid problems that come with live, interactive communications and to avoid with guest books the appearance of creating an open forum for all speakers and messages. If a district has a strong tradition of using a guest book and insists upon doing so, it should make certain that messages written by individuals other than specially designated school district personnel are reviewed for appropriateness before they are posted at the Web site.

One rendition in Congress in 1999 would require all schools receiving federally subsidized Internet hookups to install computer software to block inappropriate materials.

Filtering, monitoring & blocking the Internet

The idea of installing filters to block school networks from access to certain Internet sites that contain objectionable material has been controversial. Three types of software give school districts some control over what Internet content is accessible on their networks. *Blocking software* prohibits users from gaining access to certain sites. *Filtering software*, identifies objectionable words and phrases and blocks access to sites that contain them. *Inclusion software* allows access only to designated sites.

All three are dependent on the software program's thoroughness and adaptability to change, and all have weaknesses. For example, a program could screen out sites of potential educational value (such as one about breast cancer) because it searches mechanically for seemingly pornographic or inappropriate words. And filtering software might ban student access to information about the Mars exploration project on NASA's Web site because the URL, *http://rsd.gsfc.nasa.gov/marslife/marsexpl.htm*, contains the word "sex."

Besides the issue of protecting students from objectionable material, issues of free speech and censorship often take center stage in deciding whether to implement filtering technology. Some argue in favor of full access to "the world's largest library," while others say filtering is a useful tool that facilitates smooth use of education technology resources and reduces complaints of teachers, students and others. Each community should weigh the relative merits and come up with a policy conclusion. From a legal standpoint, currently there is not a

CENSORSHIP

Can outside organizations challenge school Internet filters that block access to pornography and other objectionable material?

Maroon High School deploys an Internet filter to censor pornography, hate material and Web sites that are not suitable for high school students. The local civil liberties group objects to censorship in any form and threatens litigation. The organization demands that the filter be removed immediately and points to cases in which public libraries have been forced to remove filters.

May the filter lawfully remain?

Answer: The filter can be lawful, although the manner in which it is implemented could cause problems. Schools may limit materials going into their libraries and classrooms if there are legitimate pedagogical concerns to support such actions. (*Board of Education, Island Trees Union Free District # 26 v. Pico*, 457 U.S. 853 1982). Similarly, schools should be able to prevent inappropriate material from arriving at school through the Internet. If the filter is ineffective and filters out harmless material, or if the filter is used to screen information based on political content of Web sites, there could be problems with its implementation.

Policy Solution: The policy and administrative regulations that authorize Internet filters should provide a strong rationale for filters – citing academic and safety concerns for children in the district's care. The best solution for legal problems with filters is to make sure the Director of Technology who oversees the filter or the company conducting the work is relying upon sound educational reasons for deciding what is filtered and is not making decisions arbitrarily.

great deal more potential liability incurred with or without the filter.[11]

For a more detailed discussion of pornography, the First Amendment, the law and the *Reno* decision, see Appendix 1.

Equal access to technology

Ideally, a school district's practice would permit children with disabilities to have equal access to the computers and other technologies commonly used by other students. Approaches that impose additional restrictions or prohibit use by disabled students could place a school district at risk of a lawsuit under Section 504 of the Rehabilitation Act of 1973 or Title II of the Americans With Disabilities Act (ADA), both of which forbid discrimination. Potential causes of action also include the Individuals with Disabilities Education Act (IDEA). [For more on this topic, see the ADA section of Chapter 2: *Administrative Issues in School Technology*. Also see *Technology for Students with Disabilities: A Decision Maker's Resource Guide*, published in 1997 by the National School Boards Association and the U.S. Department of Education's Office of Special Programs and described in the publication list at the end of this book.]

Another aspect of equal access is raised by the Equal Access Act, a federal law that requires school districts to treat religious and political groups the same as it treats other outside groups. If the district lets one organization use the Internet, e-mail or other technology, then it must grant the same favor to religious groups or to those with a point of view that might potentially be hostile to the interests of the district. If a district does allow outside groups to exchange open views at its Web site, the district should require the groups to furnish disclaimers. A group should state explicitly on its Web pages that its views, opinions and content do not reflect that of the school district.

Conclusion

Districts should adopt Acceptable Use Policies that spell out the purposes for which students may use the school's Internet connection. AUPs should indicate that students should only access appropriate Web sites and that students may be disciplined for accessing pornographic or indecent material. No one policy fits all. It is important for the school district to consider its size, how computers are used in education, what problems have occurred in the past, and how vigorously the finer details of the policy will be enforced.

The Internet is truly a remarkable technology for educating students. If used properly, it can enhance the learning experiences of students of all ages. Because the Internet enables such a dynamic environment, and because state and federal legislatures are constantly changing the laws that govern access to material there, school districts must give careful and continuing thought to its implementation and take actions that balance protection with Internet access.

Ronald D. Wenkart is General Counsel for the Orange County Department of Education in Costa Mesa, California. He supervises a legal staff that represents 28 school districts, five community college districts, four Regional Occupational Programs, the Orange County Superintendent of Schools and the Orange County Board of Education. He has represented schools in the state of California since 1978.

Edwin C. Darden is staff attorney for the National School Boards Association and editor of this publication. He is knowledgeable about a wide range of education law topics, and teaches classes on the subject.

11. For more information on filters, see two books: *A Practical Guide to Internet Filters* and *Shining A Light on Filters in Libraries*, both by Karen G. Schneider, MSLIS. Schneider managed "The Internet Filter Assessment Project," a librarian project that ran from April to September, 1997. The purpose was to take a hard look at Internet content filters from a librarian's point of view. More than 40 librarians from around the world participated. Some were filter proponents and some were not. *See http://www.bluehighways.com/tifap.*

Elements of an Effective Acceptable Use Policy (AUP) Governing Student Internet and Technology Access

1. Establishes clear parameters and detailed ground rules on when and how students can use the Internet – whether at school or at home.

2. (a) Contains an annual notification clause that requires parents or guardians at the start of each school year to affix their signature to a user agreement, which grants explicit permission for their child to use the school-provided Internet service. Schools should also require the student's signature on the same or a separate document. Both should acknowledge that the policy has been read, understood and will be obeyed.

   (b) An alternative approach would be to use a clear, straightforward notice sent home to outline expectations and to warn parents that there is a possibility of encountering offensive and inappropriate material. The notice would acknowledge that despite prudent, reasonable and best efforts, the district is unable to absolutely preclude access to such material.

   (c) A third option, an perhaps the safest, is to do both. Send home a general notice stating the risks of technology and the responsibilities of the district to take reasonable efforts to make sure students use it in a safe and responsible manner, but also have a permission slip – with the Acceptable Use Policy attached – that students and parents are expected to sign.

3. Asserts the rights of the school district to limit the content of material that students read due to legitimate pedagogical concerns.

4. Explains to parents that, as with other matters, teachers and administrators will supervise the conduct of the children on school grounds and enforce rules and regulations necessary to their protection. The policy should also contain a statement that enlists parent support for enforcement.

   For example, The Eugene, Oregon, "E-mail and the Internet" policy states "Although student use of the Internet while at school will be supervised by staff, we encourage parents to have a discussion with their children about values and how those beliefs should guide student activities while using the Internet."

5. Makes compliance part of the student code of conduct and subjects students to discipline for willful violations.

6. Prohibits obscenity and other offensive language while using school equipment.

7. Makes reference to applicable copyright laws and pledges compliance with them as part of student use.

8. Prohibits use of school provided Internet access by students for commercial or financial gain.

9. Forewarns students that network administrators can review e-mail, file folders and communications to maintain system integrity and insure that users are using the system responsibly. Users should not expect that files stored on district servers are private.

10. Is accompanied by detailed regulations to help school personnel implement the intent of the policy.

11. Imposes personal responsibility for passwords, security and maintenance of equipment. The policy should stress that password sharing, for example, is strictly prohibited.

12. Includes specific punishments for violations of the policy. Also, the policy should deal severely with hacking or damage to files and computers. One approach is to provide a detailed list of prohibited activity and then include catch-all language for unanticipated and inventive student misbehavior.

13. Is accompanied by or includes a "netiquette" document that guides users as to proper decorum while using the Internet, e-mail or other electronic communications.

14. Warns against credit card fraud, electronic forgery or other forms of illegal behavior.

15. Forbids students from scanning in images of their own accord.

16. Specifies whether chat rooms and sites selling term papers, book reports and other forms of student coursework will be considered off limits.

17. Asserts that the school district will not be responsible for unauthorized costs incurred by students, nor will the district vouch for the accuracy of information obtained through the Internet, nor will the district be responsible for students' negligence or mistakes.

SAMPLE ACCEPTABLE USE PREAMBLE

The following is a fine example of a preamble to an acceptable use policy. The first paragraph is a statement of purpose. The second outlines the risks but reaffirms the district's commitment to the value of technology in education. The final paragraph gives a general statement of expectations.

The Plano Independent School District provides technology resources to its students and staff for educational and administrative purposes. The goal in providing these resources is to promote educational excellence in the Plano schools by facilitating resource sharing, innovation, and communication with the support and supervision of parents, teachers, and support staff. The use of these technology resources is a privilege, not a right.

With access to computers and people all over the world comes the potential availability of material that may not be considered to be of educational value in the context of the school setting. Plano ISD firmly believes that the value of information, interaction, and research capabilities available outweighs the possibility that users may obtain material that is not consistent with the educational goals of the district.

Proper behavior, as it relates to the use of computers, is no different than proper behavior in all other aspects of Plano ISD activities. All users are expected to use the computers and computer networks in a responsible, ethical, and polite manner. This document is intended to clarify those expectations as they apply to computer and network usage and is consistent with district policy.

– Plano Independent School District, Texas

Resources

The following Web resources are presented as a convenience to the reader. With the rapid changes that occur every day in cyberspace, this book's editors can assure only that the sites were "live," accessible and useful at the time of publication.

See the following Web sites for sample Acceptable Use Policies and observations about technology. Some AUPs address whole school communities; others target only students, faculty or other specific groups. Your state school boards association and department of education may offer additional sample polices.

A Legal and Educational Analysis of K-12 Internet Acceptable Use Policies – by Nancy Willard, Eugene, Oregon
http://www.erehwon.com/k12aup/legal_analysis.html

Intellectual Freedom in Cyberspace, Resources for Librarians and Educators
http://metronet.lib.mi.us/ROCH/freedom.html

Critiquing Acceptable Use Politices – by Dave Kinnaman
http://www.io.com/~kinnaman/aupessay.html

Sample AUPs at Rice University
http://www.rice.edu/armadillo/acceptable.html

Acceptable Use Policies of Internet Service Providers
http://www.jmls.edu/cyber/statutes/email/policies.html

Acceptable Use Policy for Newport-Mesa Unified School District and Other California Districts
http://www.nmusd.k12.ca.us/Resources/Policies.html

Developing a School or District Acceptable Use Policy for Student and Staff Access to the Internet – by Clancy J. Wolf, Bremerto, Washington
gopher://inspire.ospi.wednet.edu:70/00/Accept_Use_Policies/IN_policies.txt

Acceptable Use Policies Compiled by Web66, the University of Minnesota
http://mustang.coled.umn.edu/Started/use/Acceptableuse.html

Schools, the Internet and the Law: Legal and Policy Concerns for Schools Using the Internet – by David E. Sorkin, the John Marshall Law School (presentation outlines)
http://www.mcs.net/~sorkin/internet/

Pitsco Acceptable Use Policies
http://www.pitsco.com/p/resframe/htm

Massachusetts Association of School Committees
http://www.masc.mec.edu/aupfax.html

California School Boards Association
http://www.csba.org/ps/samintro.htm

INTERNET FILTERING, BLOCKING & MONITORING PRODUCT WEB SITES

ITech Inc., AUP Action Tools
http://www.aupaction.com

N2H2 Inc.
http://www.n2h2.com

Novell
http://www.novell.com/bordermanager

CyberPatrol
http://www.cyberpatrol.com

Security Software Systems, Inc.
http://www.securitysoft.com

CYBERsitter
http://www.solidoak.com/cysitter.htm

Cyber Snoop
http://www.pearlsw.com/csnoop/snoop.htm

GuardiaNet
http://www.guardianet.net

UR Labs
http://www.urlabs.com/public

Internet Products, Inc.
http://www.internetProducts.com/products

Sequel
http://www.sequeltech.com/products

Net Nanny
http://www.netnanny.com

Net Shepherd
http://www.netshepherd.com

NetSnitch
http://www.netsnitch.com

AbirNet
http://www.abirnet.com

Secure Computing
http://www.securecomputing.com

surfCONTROL
http://www.surfcontrol.com

SurfWatch
http://www.surfwatch.com

Innovative Protective Solutions, Corp.
http://www.ips-corp.com/tripleex.htm

Web Chaperone
http://www.webchaperone.com

NetPartners Internet Solutions
http://www.websense.com

WizGuard Corporation
http://www.wizguard.com

X-Stop
http://www.xstop.com

Sample documents

STUDENT ACCEPTABLE USE CONSENT FORM

****

STUDENT

Name _____ Grade _____

School _____

I understand that my computer use is not private and that the school district will monitor my activity on the computer system.

I have read the school district's electronic communications system policy and administrative regulations and netiquette guidelines and agree to abide by their provisions. I understand that violation of these provisions may result in suspension or revocation of system access.

Student's signature _____ Date _____

PARENT/GUARDIAN ACCEPTABLE USE CONSENT FORM

****

PARENT OR GUARDIAN

___ I do not give permission for my child to participate in the school district's electronic communications system.

****

I have read the District's electronic communications system policy, administrative regulations and netiquette information. In consideration for the privilege of my child using the district's electronic communications system, and in consideration for having access to the public networks, I hereby release the school district, its operators, and any institutions with which they are affiliated from any and all claims and damages of any nature arising from my child's use of, or inability to use, the system, including, without limitation, the types of damage identified in the school district's policy and administrative regulations.

___ I give permission for my child to participate in the school district's electronic communications system and certify that the information contained on this form is correct.

Signature of parent or guardian _____

Home address _____

Date _____ Home phone number _____

Chapter 2

Administrative Issues in School Technology

Rodney A. Satterwhite, Calvin S. Spencer, Jr. and R. Craig Wood*
McGuire Woods Battle & Boothe LLP
Richmond and Charlottesville, Virginia

Introduction

As President Clinton has stated, "Preparing our children for a lifetime of computer use is now just as essential as teaching them to read and write and do math. ...We must make technological literacy a standard." Statistics bear out the need for this policy. By the year 2000, 60 percent of all jobs in the United States will require information technology skills, and that percentage is expected to continue to increase. Research and experience suggest that when technology is used effectively in education, it can positively enhance students' educational attainment and skills acquisition.

Along with the benefits of technology in schools come a host of legal and practical implications for school boards and administrators. This chapter addresses school district liabilities in such matters as sexual harassment, the Year 2000 problem and universal access for individuals with disabilities. It also sorts out issues with e-mail and the very real possibility that school employees will be forced to turn incriminating information over to the other side in the course of a court case. The chapter also addresses attorney-client privilege in electronic communications and the obligation of school board members to restrain from inadvertently violating their state's open meetings law while enjoying the ease and convenience of electronic communications.

School district liability for electronic communications

By the year 2000, an estimated 40 million users will send 60 billion e-mail messages a year. Students and teachers are increasingly proficient in the use of e-mail and often rely on it as a primary source of communication. At its best in the education field, e-mail provides a forum for students and teachers to interact and exchange academic-related ideas. At worst, e-mail can be a costly waste of human resources and a tool of harassment and discrimination.

The increased use of communications technology by administrators, teachers and

* *A biographical sketch of the authors is available at the end of this chapter.*

1. California State Department of Education, 1996.

students exposes school districts to potential legal liability and practical difficulties in a number of ways. Many existing claims, such as sexual harassment, wrongful discharge and discrimination, take on a new light when the computer is the medium for the wrongful behavior, or when electronic communications are used as evidence.

SEXUAL HARASSMENT

E-mail no longer consists of text alone. Users now have the capability of sending and opening attachments with pictures and voice recordings. Unfortunately, some users send pornographic pictures or obscene recordings as attachments to unsuspecting readers. For example, an administrator might send a pornographic e-mail joke or an e-mail with an attached pornographic picture to an unsuspecting teacher. Without appropriate safeguards, a school district could be held liable for such actions.

A sexually hostile work environment claim may arise from conduct that has the purpose or effect of unreasonably interfering with an individual's work performance or creating an intimidating, hostile or offensive work environment.[2] Under Title VII of the Civil Rights Act of 1964, even verbal or written conduct can give rise to a "hostile environment" claim if it is sufficiently severe and pervasive to alter an employee's working conditions.

The inquiry in these types of claims often focuses on what type of improper behavior constitutes severe and pervasive conduct. In *Harley v. Coach*, 928 F. Sup. 533 (E.D. Pa. 1996), a racial harassment case that is analyzed under the same rules as sexual harassment cases, the court addressed this issue. The court held that one e-mail containing a racial epithet, a racial slur uttered by a supervisor and teasing by a co-employee, were not sufficient to create a racially hostile work environment. The court relied on a Third Circuit Court of Appeals opinion, *Drinkwater v. Union Carbide Corp.*, 904 F.2d 853, holding, "the comments . . . are insufficient in and of themselves to support a hostile environment claim. Hostile environment harassment claims must demonstrate a continuous period of harassment, and two comments do not create such an atmosphere." These cases indicate that in some instances occasional, sporadic use of inappropriate e-mail may not constitute sexual harassment. However, the inquiry is a fact-based one, and it is within a court's power to find sexual harassment where it deems the conduct sufficiently egregious. Therefore, schools must institute strong policies against sexual harassment to prevent improper conduct, including in electronic communications, and take adequate remedial measures when it does occur.

Persistent offensive e-mails by (1) an administrator to a teacher; (2) a teacher to another teacher; (3) a teacher to a student; or (4) a student to a student can support a hostile environment claim[3] and the standard of liability that applies in each case varies. The standard for finding a school liable for sexual harassment by its employees differs depending on whether the victim is an employee or a student.

Where a teacher or staff member alleges that an administrator is the harasser, vicarious liability principles apply. In other words, the school district may be held legally responsible for a hostile environment created by a supervisor with authority over the employee.[4]

Recent Supreme Court decisions allow an employer to escape paying money damages only where two elements are present: (1) evidence the employer exercised reasonable care to prevent and promptly correct sexually harassing behavior *and* (2) evidence the employee failed to take advantage of corrective opportunities available to

2. *See Harris v. Forklift Systems, Inc.*, 114 S.Ct. 367 (1993).

3. Several states, including Minnesota and California, have enacted legislation prohibiting sexual harassment in schools.

4. *See Burlington Industries, Inc. v. Ellerth*, 118 S.Ct. 2257, 2270 (1998).

the employee.[5] This standard is fairly strict, and unless schools take strong preventive measures they may not be able to prevent future liability. Schools must take special care in hiring and monitoring supervisors; implement a clear, specific and comprehensive sexual harassment policy with well-defined complaint procedures; and disseminate and periodically review the policy with all employees.

The legal standard changes somewhat where a teacher sexually harasses a student. The United States Supreme Court has held that a school district may be held liable under Title IX for a teacher's sexual harassment of a student.[6] The Supreme Court recently ruled in *Gebser v. Lago Vista Ind. Sch. Dist.*, 118 S.Ct. 1989 (1998), however, that the school district may be held liable only if a school district official with authority to institute corrective measures on the district's behalf has *actual notice* of, and is deliberately indifferent to, the teacher's misconduct.

Courts are split as to whether a school district can be held liable for student to student harassment.[7] Courts finding school districts liable for such harassment have imposed the same "actual notice" requirement that the Supreme Court applied in *Gebser*. This issue is pending before the United States Supreme Court as this chapter goes to print.

While a court may find that a school district is not legally responsible for sexual harassment by a student or teacher, deterring offensive conduct is cheaper and more productive than defending against a lawsuit. The institution of an e-mail policy helps to provide an affirmative defense for a school district being sued in a sexual harassment case. Under such a policy, all users should be required to review and sign an Acceptable Use Policy statement that includes prohibition of online sexual harassment and indicating their agreement to comply with its provisions. If a district becomes aware of the sexual harassment of a student or teacher via e-mail, the district must take immediate steps to halt the harassment, including limiting the offender's use of e-mail privileges, or risk being held liable for sexual harassment. Similarly, if a teacher or administrator becomes aware of a student's misuse of e-mail privileges, those privileges should be restricted or terminated. As a further measure to deter sexual harassment suits related to e-mail misuse, a district should issue guidelines for reporting e-mail misuse.

DISCRIMINATION CLAIMS

Just as e-mail may be a tool for sexual harassers, it may also provide fertile ground for discrimination claims ranging from age and disability discrimination to racial and gender discrimination.[8] For example, a teacher may use e-mail to send racially offensive jokes to other teachers. Or an administrator may send offensive e-mails relating to the termination of an employee, providing ammunition for a later age discrimination or disability discrimination claim. Such electronic communications could form the primary evidence in a discrimination case.

School districts should think carefully about access issues and potential claims of differential treatment by students or employees. An equitable approach to technology in the school district should allow schools to shake off adverse litigation at an early stage.

---

5. *Id.*

6. *See Franklin v. Gwinett County Pub. Sch.*, 503 U.S. 60, 63 (1992).

7. *Compare Rowinsky v. Bryan Indep. Sch. Dist.*, 80 F.3d 1006 (5th Cir. 1996), cert. denied, 117 S.Ct. 165 (1996) *and Doe v. Petaluma City Sch. Dist.*, 949 F.Supp. 1415 (N.D.Cal. 1996) *with Bruneau v. South Kortright Cent. Sch. Dist.*, 962 F.Supp. 301 (N.D.N.Y. 1997).

8. *E.g., Wilson-Simmons v. Lake County Sheriff's Dept.*, 982 F. Supp. 496 (N.D. Ohio 1997); *Keppler v. GPU, Inc.*, 2 F. Supp. 2d 730 (W.D. Pa. 1998); *Strauss v. Microsoft Corp.*, 856 F. Supp. 821 (S.D.N.Y. 1994).

Use of e-mail in litigation

Parties entrenched in litigation or facing potential litigation have an ongoing duty to preserve information they know is going to be relevant. E-mail, then, creates a tremendous amount of potentially discoverable information in litigation.

In the discovery phase of litigation, one side digs for information from its opponent by asking written questions and conducting face-to-face interviews. Attorneys are bound by ethics and law to turn over the requested information, even if it is incriminating or harmful to their case.

In modern litigation, attorneys frequently demand the production of relevant e-mail. Because of its informal nature, attorneys consider e-mail an excellent source of discovery and potential evidence for use at trial. Frequently, administrators and teachers make statements on e-mail that would not be placed into written memos or documents.

Although case law on e-mail as evidence in employment litigation is somewhat sparse, employers can look for increased use of e-mail as primary evidence in sexual and racial harassment cases. In *Knox v. Indiana*, 93 F.3d 1327 (7th Cir. 1996), for example, a state employee sued for sexual harassment based in large part on e-mail messages sent to her by her supervisor. The supervisor's messages propositioned the plaintiff for sex, and the plaintiff's investigator discovered those e-mails. The United States Court of Appeals for the Seventh Circuit affirmed a jury verdict for the employee based on her Title VII claims.[9] Moreover, with the increased ability to attach pornographic images to e-mail messages, employers likely will see more sexual harassment suits by employees who are exposed to the display of pornographic or other offensive material.

DISCOVERY OF ELECTRONIC COMMUNICATIONS

E-mail messages are now as easily discoverable as paper messages have always been. Federal discovery rules provide that the word "document" includes electronic "data compilations,"[10] and courts interpreting the Federal Rules of Civil Procedure have held that e-mails are subject to the same discovery rules as documents.[11] Courts have also punished employers for deleting e-mails, after the initiation of litigation, that might have been useful to the adverse party at trial.[12]

"To prevent the use of e-mail adverse to school districts in litigation, districts should institute e-mail use policies and uniformly enforce e-mail use restrictions."

To prevent the use of e-mail technology in ways that could be adverse to school districts in litigation, districts should institute e-mail use policies and uniformly enforce e-mail use restrictions. First, a policy prohibiting or severely limiting personal use of e-mail should be implemented to deter improper use and help shield a district from liability relating to such use.

9. *See also Vicarelli v. Business Int. 'l Inc.*, 973 F. Supp. 241 (D. Mass. 1997).

10. The Federal Rules of Civil Procedure provide that documents include "writings, drawings, graphs, charts, photographs, phone records and other data compilations from which information can be obtained, translated, if necessary, by the respondent through detection devices into reasonably usable form . . ." Fed. R. Civ. P. 34(a).

11. *See In re Brand Name Prescription Drugs Antitrust Litigation*, 1995 WL 360526 (N.D.Ill. 1995) (unpublished disposition).

12. *See Proctor & Gamble v. Haugen*, 179 F.R.D. 622 (D. Utah 1998).

Ways to prepare for e-mail discovery in litigation

1. Create and enforce an electronic document policy that minimizes the amount of time the information is stored.
2. Enforce the policy in a uniform way. Do not deviate when faced with litigation or potential litigation.
3. When working with the school attorney, create a litigation response that includes a process for preserving relevant data at the outset of litigation.
4. Do a litigation risk assessment that identifies weaknesses and strengths and potential high-cost areas.
5. Educate employees and emphasize the need for a business approach to e-mail communications.
6. For safety's sake, both the attorney and client should assume that their e-mail will have to be produced in discovery. Thus, unusually sensitive communications should not take place via this medium.

Second, a district should develop a policy regarding preservation of e-mail files. Some government agencies do not back-up e-mails at all to avoid inadvertent retention problems. Whatever a school district's policy, it should be adhered to at all times, including upon request for discovery of e-mails. If a district's policy is to delete e-mail files every month, it may not deviate from that policy to defeat discovery by deleting every week. Moreover, once a discovery request has been made, school districts have a duty to refrain from deleting e-mails even if it would normally do so under its own policy. Having a fairly short time frame for e-mail retention is advisable in terms of discovery or liability. E-mail users can be encouraged to print out and save paper copies of documents important to them. Anything of great significance is then committed to paper or recalled through the memory of witnesses.

Courts have not extended a sympathetic ear to arguments of undue expense and burden in the context of discovery and demand for e-mail production. Thus, having a policy and a systematic way of proceeding on such matters avoids the potentially cumbersome and expensive process of finding an e-mail on demand. In one Ohio case, for example, a federal district court refused to grant relief to a plaintiff who asserted that such a request would require a search of 2.8 million documents, cost more than $80,000 and require hundreds of hours. The court said the request for relevant documents was reasonable and the burden was the result of the party's own unwieldy record-keeping system. Further, the court said: when a party chooses electronic storage for information, the need for retrieval is an "ordinary and foreseeable risk."

The duty imposed on entities to preserve e-mail was illustrated in a case involving Proctor & Gamble (P&G) and Amway – fierce competitors in the personal care and home care market. In the midst of a lawsuit, P&G served Amway with broad discovery documents that demanded access to e-mail correspondence. The problem was, it failed to retain its own e-mail files for Amway's discovery purposes. The court, illustrating the point that the practice was unacceptable, forced

P&G to pay Amway $10,000, saying P&G's routine practice of purging its e-mail daily (because of the pending lawsuit) was a violation of the federal rules of discovery.

SECURITY ISSUES

Because the attorney-client privilege is based in part on the expectation of privacy in communications, the increasing use of technology raises concerns about privileged communications. Generally, the attorney-client privilege extends to (1) a communication from a client (2) to the client's lawyer or the lawyer's agent (3) relating to the lawyer's rendering of legal advice (4) made with the expectation of confidentiality and (5) not in furtherance of a future crime or tort, provided the privilege has not been waived.

The fourth element, an expectation of confidentiality, has particular relevance to e-mail correspondence. If the client does not treat the information as confidential, the client will not have an expectation of privacy and the privilege may never arise. In *Bowne of New York City, Inc. v. AmBase Corp.*, 150 F.R.D. 465, 491 (S.D.N.Y. 1993), the court held that the disclosure of attorney confidences to corporate employees for purposes unrelated to the obtaining of legal services from the corporation's attorneys vitiates the privilege. It warned, "[i]f a corporation wants the benefits of the privilege it should enforce a fairly firm 'need to know' [policy] of the communication rule."[13] In other words, forwarding e-mail messages to unnecessary recipients can destroy the confidentiality element needed to maintain the privilege.

13. See also *Jonathan Corp. v. Prime Computer, Inc.*, 114 F.R.D. 693, 696 (E.D. Va. 1987) ("It should be noted, however, that by virtue of Prime's failure to indicate on the face of the memorandum that the document was confidential or contained attorney-client privileged information, coupled with the fact that the memorandum was distributed to six (6) employees, this court has serious doubts as to whether [the party] has met its burden of demonstrating that the document was intended to be confidential.")

IMPACT OF UNSECURED TECHNOLOGY ON THE ATTORNEY-CLIENT PRIVILEGE

When communications occur in circumstances where others can easily overhear, there is no expectation of confidentiality. The advent of technology that can be intercepted easily broadens the possibility of waiver of the privilege. For example, a cordless telephone is a two-way radio transmitter/receiver. Anyone within 1,000 feet who is listening with a scanner, compatible cordless telephone or other radio receiver can intercept the conversation. Although it is a violation of federal and state law to intercept cellular telephone conversations, the Illinois State Bar Association has held that persons using such phones do not have an expectation of confidentiality.

Similarly, e-mail communications via the Internet may not enjoy the privacy protections one expects from an employer-operated e-mail system. Unlike private e-mail systems, the sender of an Internet e-mail message has no control over the routing, storage or access to the message either in transit or at the receiving address. Although very little case law exists on the subject, courts likely will refuse to find an expectation of privacy for e-mail sent over the Internet.

Advisory opinions issued by attorney bar groups in several states engage in a more detailed analysis of the issue. The prevailing approach of these opinions is that unencrypted e-mail to attorneys on routine matters carries with it the assurances of confidentiality, but highly sensitive matters require enhanced security. In an opinion released February 12, 1998, the District of Columbia Bar Legal Ethics Committee determined that except in extraordinary circumstances, unencrypted e-mail is an acceptable form of conveying client confidences, even where the lawyer does not obtain prior consent from the client. In addition, a 1998 law in New York state added to the Civil Practice Law and Rules to

ensure no attorney-client communication would lose its privileged status solely by virtue of being communicated by electronic means.

Keep in mind these same general principals that are considerations for dealings with outside counsel are equally applicable to communications that flow through the in-house school district legal department.

PRECAUTIONS

As a precaution to the waiver of attorney-client privileged information, school districts should inform administrators about the rules surrounding the expectation of confidentiality. Armed with legal rules, administrators will be better able to take the practical precautions necessary when communicating with counsel. School districts also may wish to consider the use of encryption technology. Encryption is a method of scrambling electronic mail messages at their source so that anyone who intercepts messages will be unable to read them. The intended recipient of the messages will have a corresponding decryption utility that renders the messages readable. Commercial and shareware encryption utilities are readily available.

School board use of e-mail as a public meeting: state Sunshine Laws

With the rapid advancement in the technology of electronic communications has come the need for state legislatures to revise their Open Meetings Laws. These laws (commonly referred to as Sunshine Laws) generally require that meetings of school boards and other public bodies be conducted openly, so all interested persons are permitted to attend and listen to deliberations and proceedings. The policy behind these laws is the assurance that the public has access to information concerning the way the government conducts the public's business. But laws differ from one state to another.

The increased use of e-mail, virtual conferencing and other forms of interactive communication have created uncertainty in government agencies, including school boards, about whether such communications violate Sunshine Laws. When one board member sends an e-mail to other members about school board business, does that violate the state's Sunshine Law? What if the members are using a simultaneous interaction (such as live chats) rather than a serial one? How about when board members use e-mail, telephones or faxes to poll one another about board issues? While one might think these instances would be analogous to the use of telephones by board members, the issues are often more complicated.

Elected officials, therefore, should be cognizant of the requirements of their state's open meetings law and adhere carefully to its dictates. When in doubt, board members should avoid sending e-mails to everyone to poll fellow colleagues about public issues. A single e-mail copied to fellow board members or separate e-mails to each board member on a single public topic are roughly equivalent – and both could violate open meetings laws. For the same reason, board members should be cautious in using live, interactive technology to have a simultaneous electronic interchange of opinions.

No case involving the use of e-mail as a public meeting has reached the courts, but state legislatures and state attorneys general are pursuing clarification of the issue. A 1995 Kansas Attorney General's Opinion found school board members may be in violation of the state Sunshine Law if a quorum of "board members *simultaneously* engage[s] in discussion of the board business through computer terminals."[14] The Kansas Sunshine Law defines "meeting" to include any "gathering, assembly, telephone call or any other means of *interactive*

14. Kan. Atty. Gen. Op. No. 95-13, 1995 WL 40761 (Kan. A.G.) (Emphasis added). Open Meetings Law: K.S.A. 75-4317a.

communication."[15] The attorney general opined that if "a sender of a message does not get an immediate response from a receiver, the communication is not *interactive.*" Simply sending a message to other board members would not constitute an 'interactive communication' as defined by law.[16]

A 1998 Kansas Attorney General opinion on open meetings went further, declaring that a series of meetings, each of which involves less than a majority of a quorum, but collectively totaling a majority of a quorum, at which there is a common topic of discussion of the business or affairs of that body constitutes a meeting for purposes of the Kansas Open Meetings Act.[17] An example would be a communication tree in which the chair e-mails board members one by one and asks their opinion on a controversial topic. In that case, no more than two board members would be "speaking" to each other at a time, but the survey would violate Kansas law. Similarly, the AG said, if one board member e-mails another, who adds to the e-mail and sends it along to the next, that would violate the law. The same would be true of a group mailing list in which each member automatically receives messages posted by others, and can comment on the messages. This would be circumventing the law, according to the opinion, because members could exchange their thoughts on an issue without ever gathering or communicating in real time.

Compare the Kansas opinion, however, to *Del Papa v. Board of Regents of the University and Community College System of Nevada.*[18] In *Del Papa*, the Nevada Supreme Court held, "a quorum of a public body using *serial communication* to deliberate toward a decision ... on any matter over which the public body has supervision" violates the state's Sunshine Law.[19] In that case, the chairman of the school board sent faxes to board members requesting their opinions about whether to issue a media statement condemning public criticism of school board activities by one of its members. All board members received faxes except the member who had made public criticisms. The board members responded to the chairman's inquiry by telephone, and the chairman ultimately decided not to issue the media statement.

In finding the school board violated the state Sunshine Law by using telephones and faxes to transact school board business, the court based its analysis on the definition of "meeting." The court also relied on case law in other jurisdictions holding that the making of decisions by public bodies using either telephone or mail polls without public attendance constitutes a meeting and therefore violates the spirit of the state's Sunshine Law. Finally, the court relied on a provision in the state code declaring that "electronic communication ... must not be used to circumvent the spirit or letter of the [Sunshine Law]."[20]

The varying conclusions in these decisions illustrate the disparity among state laws in this area. A survey of state Sunshine Laws suggests some states still operate under old Sunshine Laws and make no mention of electronic communications, while others have amended their statutes to include such provisions.

To determine whether board members have complied with a state's Sunshine Law, courts will also review the substance of the communication that occurred. Once again, the determination depends on the language of the statute at issue, but most statutes prohibit private communications among board members only where "public business" is being transacted. Public business usually includes the adoption of any proposed policy, resolu-

15. *Id.*

16. *Id.*

17. Kan. Atty. Gen. Op. No. 98-26 (April 20, 1998).

18. 956 P.2d 770, (Nev., 1998).

19. *Id.* at 778.

20. *Id.* at 773.

EXCERPTS FROM STATE SUNSHINE LAWS

California — Amended its Sunshine Law in 1994 to define "meeting" as "... any use of direct communication, personal intermediaries, or technological devices that is employed by a majority of the members..."[21]

Montana — The term "meeting" is now defined as "the convening of a quorum ... whether corporal or by means of electronic equipment to hear, discuss or act upon a matter...."[22]

Colorado — Defines "meeting" as "any kind of gathering convened to discuss public business, in person, by telephone, electronically, or by other means of communication."[23]

Virginia — The state Freedom of Information Act provides that any governing body conducting a meeting where the "public business is discussed or transacted through telephonic, video, electronic or other communication means where the members are not physically present" violates the law.[24] These varying statutes demonstrate the need for public officials to be well informed about the laws in their state.

21. Cal. Govt. Code Ann. §54952.2 (West, 1998).
22. Mont. Code Ann. §2-3-202 (West, 1997).
23. Col. Rev. Stat. Ann. § 24-6-402 (West, 1998).
24. 1950 Va. Code Ann. §2.1-343.1. (Michie, 1998).

tion, rule or other formal action.[25] It might also include deliberations on those same matters.

Many state Sunshine Laws and "Public Records Acts" require public access to certain records. Again, statutes vary widely, but most require that records documenting policies, decisions, procedures and other operations of public offices be made available to the public. The issue for schools and other public agencies is whether e-mail communications between board members constitute *public records* for purposes of state law.[26] This inquiry raises many difficult questions. Should all e-mail communications be archived as is required of other documents? How well are public agents equipped to act as official custodians of such communications and to determine whether or not they are public records?

[For a discussion of e-mail, student records and the Family Educational Rights and Privacy Act (FERPA) see Chapter 1: *School District Policies for Student Use of the Internet & Electronic Publication of Student Works*. For a discussion of e-mail records and litigation, see this chapter above. For a general discussion of e-mail records and employees, see Chapter 3: *Legal Considerations in Regulating Employee Use of School Technology*.]

The Colorado Legislature attempted to address these issues in its Sunshine Law.[27] That statute specifies only e-mail used "to discuss pending legislation or other public business" shall be subject to the Sunshine Law, and state law does not cover e-mail communications about any other topics.[28] While such legislation may give some guidance to state agents in determining whether communications are covered by law, the language is still vague and open to interpretation by courts.

In passing legislation to clarify the use of e-mail as public records, legislatures must engage in balancing the policy of providing wide access to government information and activities against the privacy interests and practical limitations of public officials and employees.[29] E-mail is a useful tool for state officials to gather information and communicate with staff, other officials, agencies and the public. Legislatures are challenged with trying to

25. *See* Col. Rev. Stat. Ann. § 24-6-402. 2(c)(West, 1998).
26. *See generally, State v. Lake County Sheriff's Department*, 693 N.E.2d 789 (Ohio, 1998).
27. Col. Rev. Stat. Ann. § 24-6-402.2(d)(III). (West, 1998).
28. *Id.*
29. Col. Rev. Stat. Ann. § 24-6-402 (West, 1998).

protect such communications while also protecting public access to public information.

These materials demonstrate that as technological communications continue to advance, school board members will have to adjust their behavior. In some jurisdictions, individual e-mail communication among board members may not violate state law, while in others it may be a clear violation. Other forms of interactive communication (such as virtual conferencing, chat rooms and instant messaging systems) accentuate the need for school board members to recognize the implications of all forms of board communication. Members should be familiar with state laws governing such communications, and where uncertainty exists they should seek the advice of counsel. Since most statutes provide for the nullification of board decisions that violate state Sunshine Laws, school board members would be well advised to take preemptive action to determine what types of communication are implicated by law.

The Year 2000 problem

The Year 2000 problem, commonly known as the "Y2K problem," is a legitimate threat to the technology operations of nearly every school district in the United States. To conserve computer memory, save time and money, and simplify numerical input procedures, many hardware and software manufacturers and programmers traditionally have used only two digits (rather than four) to specify the year portion of dates entered into computer codes. Unless programs are converted to recognize the 21st century date change, those computers and software programs will interpret the year "00" as the year 1900, not 2000.

It should be said at the outset that the Year 2000 problem is multi-faceted and fraught with legal pitfalls. This section is intended to be a cursory overview of the subject, not the definitive text. In addition to considering the issues raised here, a school district would be wise to consult with appropriate technical and legal advisors to develop a specific plan tailored to its needs.

Any computer or system manufactured or programmed during the past four decades may be affected by the Y2K problem. Many school districts computerize student records, class scheduling records, personnel and payroll procedures, and bus routing records. Moreover, fire and security systems, heating and air conditioning (HVAC) systems, timers for lights, video recorders, voice mail, elevators, school bells and other systems and devices may also be computer-operated. Failure to correct Y2K coding problems in operating software could lead to failure of these functions. If relevant data is stored on a machine with older software, school districts may experience severe technological difficulties on January 1, 2000, and beyond.

The cost and time necessary to fix the Y2K problem is staggering. Taxpayers will pay more than $5 billion to correct the Y2K problem for federal government computers. The Los Angeles School District alone has almost 24.4 million lines of computer code to correct.[30] Prompt recognition of potential Y2K disruptions will allow school districts to make the necessary adjustments and achieve a smooth transition to the next millennium. Taking steps to assure Y2K compliance is not only good policy, but will avoid costly and unnecessary litigation surrounding system failures and other shortcomings associated with the computer changeover.

PERFORMING A TECHNICAL AUDIT — THE PROACTIVE APPROACH

A school district's first action in combating the Y2K problem should be to conduct a Y2K technical audit. An initial assessment of all computerized systems will provide the school district with information about potential internal problem areas.

The technical audit should include five primary steps:

1) *Awareness.* Focus the school district's energies on defining the problem, assessing management

30. The United States Department of Education is engaged in a Year 2000 compliance program. For more information on the DOE's plan to combat Year 2000 problems, see the DOE Internet web page at *www.ed.gov/offices/OCIO/year*

capabilities and obtaining district-wide support for the program. Develop a contingency plan to combat worst case scenarios such as the malfunction of fire and alarm systems, payroll software and HVAC systems.

2) *Assessment.* Identify mission-critical systems, create a vendor management team, inventory hardware and software systems, develop validation and testing strategies and develop contingency plans for mission-critical applications.

3) *Renovation.* Fix the problems by converting, replacing or eliminating hardware and software systems.

4) *Validation.* Component test each system or application. System-test the new environment prior to the last quarter of 1999.

5) *Implementation.* Track Y2K-related problems and maintain a detailed audit trail to prepare for potential litigation.

LOOKING BEYOND A TECHNICAL AUDIT

In addition to performing a technical audit, the school district should explore other Y2K-related problems. First, determine whether vendors, suppliers and service providers are Y2K compliant and can meet the district's needs in January 2000 and beyond. Even if the school district is Y2K compliant, third-party Y2K problems could directly impede the daily operations of the district. For example, Y2K failures by a payroll service or a food delivery vendor could cripple a school district's normal operations. A letter seeking verification of Y2K compliance from such suppliers and service providers will allow a school district to pinpoint potential problem areas and make alternative supply arrangements. (For a sample letter, see the joint publication by the U.S. Education Department and the Council of the Great City Schools titled *Squashing the Millennium Bug: A Year 2000 Compliance Guide for Elementary/Secondary Schools and School Districts*, published in February 1999 at *http://www.cgcs.org/Y2K12/appendix-d.htm*.

If, for example, a major material goods vendor is not compliant, the district might stockpile supplies from that vendor. If the goods are perishable or have limited usefulness, the district should consider switching vendors. If school districts are obligated to a long-term contract with a vendor whose supplies have a finite usefulness and who is not compliant, then the district needs to take all reasonable steps to gain assurances from the vendor that substantial disruption will not occur. A district may also want to look elsewhere and make other arrangements as a fallback plan.

Second, school districts should review all relevant insurance policies and determine whether coverage exists for Y2K remediation costs. When purchasing new insurance, districts might inquire about the availability of Y2K coverage and be aware of Y2K exclusions.

Third, the school district's information technology personnel should be available for service on January 1 and 2, 2000 (a weekend), and the following week. Fair Labor Standards Act overtime and compensatory time issues for these employees must be considered in advance.

Fourth, school districts should not forget about intellectual property concerns in going about their Y2K modifications. Many computer software makers prohibit any enhancement or modification without the licensor's express permission. In addition, any changes might in essence create a "derivative work" that infringes on the software owner's copyright. When embarking on a Y2K fix, districts should look to attorneys to review licensing agreements to determine what ramifications exist, if any. If outside companies are hired to make revisions, schools should be careful to hire those who have established protocols for gaining permission from copyright owners.

The final step in a school district's Y2K preparations should be a potential litigation analysis. As of December 31, 1998, at least 33

Y2K-related lawsuits have been filed in the United States.[31] Most defendants in these lawsuits are hardware and software manufacturers and programmers who developed non-Y2K compliant programs. Lawyers and software industry experts predict a flood of new Y2K litigation after January 1, 2000. If a Y2K audit process reveals serious software or hardware deficiencies that the manufacturer or vendor should have recognized, the district should contact the suppliers to request their financial and technical assistance in remedying the district's Y2K problems. If the manufacturer or service provider fails to remedy the problem, the district may choose to contact an attorney to discuss possible legal action.

"Schools must provide reasonable accommodation to individuals with disabilities unless doing so would result in a fundamental alteration to the program or service or create an undue burden on the school."

In addition, the U.S. Department of Education has dedicated a section of its Web site to the Y2K problem (*http://www.ed.gov/Y2K*). The previously mentioned guide, *Squashing the Millennium Bug: A Year 2000 Compliance Guide for Elementary/Secondary Schools and School Districts*, contains a 57-point checklist and other information to assist schools in making the transition, is included at the site and has been mailed to all 15,000 U.S. school districts.

ADA compliance for Web sites

THE ADA

According to the most recent statistics, nearly 49 million people in the United States — about one in every five people – have a disability.[32] Of those people, 4 million are children or adolescents, comprising 6.1 percent of the population under 18 years of age.[33]

To protect those with disabilities, Congress passed the Americans with Disabilities Act (ADA) in 1990. The ADA prohibits discrimination on the basis of disability in areas of employment, programs and services provided by state and local governments, goods and services provided by private companies, and in commercial facilities. The ADA also requires state and local governments to provide access to programs offered to the public. It covers effective communication with people who have disabilities and requires reasonable modifications of policies and practices that may tend to discriminate against the disabled. [For more on this topic, *see Technology for Students with Disabilities: A Decision Maker's Resource Guide*, published in 1997 by the National School Boards Association and the U.S. Department of Education's Office of Special Education Programs.]

31. Congress recently enacted the Year 2000 Information Readiness Disclosure Act, PL 105-271, October 19, 1998, 112 Stat. 2386, in an effort to provide a safe harbor for vendors and suppliers who issue Y2K compliance statements. Under the Act, a Y2K disclosure is generally inadmissible as evidence in civil actions against the maker to prove the truthfulness of a matter asserted in the Disclosure. A summary of the Act is available on the United States Congress Web site at *http://thomas.loc.gov/cgi-bin/query/Z?c105:S.2392.ENR*: Several states have passed legislation granting state agencies immunity from Y2K lawsuits.

In March 1999 the Senate was debating S.461, a bill to limit the liability of businesses whose Y2K plans do not meet expectations. The measure would limit punitive damage (punishment for economic losses) to $250,000 or three times the financial damages — whichever is greater. It would also give companies 90 days to repair the computer glitch before a suit may be filed and would allow defendants to immediately defeat a lawsuit if the company made "reasonable efforts" to remedy the situation.

Under legislation proposed in Virginia, counties, cities, towns and other political subdivisions would be immune from tort suits based on Y2K related failures. Legislative initiatives in Illinois and California to limit the tort liability of banks and software companies, respectively, have failed to pass.

32. President's Committee on Employment of People with Disabilities, 1992.

33. National Health Interview Survey, 1992.

SCHOOL COMPLIANCE

As government entities providing programs and services, public schools are covered by the Americans with Disabilities Act and must comply with its provisions. Schools must provide reasonable accommodation to individuals with disabilities unless doing so would result in a fundamental alteration to the program or service or create an undue burden on the school. Compliance includes ensuring access not only to public educational facilities, but also to communications. Whenever schools communicate information regarding their programs, goods or services, they must provide appropriate auxiliary aids or services to ensure effective communication with individuals who have disabilities. Such communications include print and audio media, as well as computerized media such as Web sites found on the Internet.

Thousands of schools in the United States and across the world have developed Web sites to provide information to the public and experience for students creating and maintaining the sites. Sites include information and links about academic programs, faculty, student organizations, parent-teacher associations, school board policies, Internet-use policies, school newspapers and even school lunches. They are an important resource for schools, and their use is rapidly increasing. Unfortunately, many schools are only beginning to realize the need to make their Web sites accessible to individuals with disabilities. Students and others with disabilities who are denied effective access to school Web pages may have a cause of action against the school under the ADA and parallel state statutes. Schools can preempt such action by being proactive in establishing universal access to all sources of communication including Web sites.

WHAT IS THE PROBLEM?

The problem for schools and other institutions is that Web sites that are perfectly accessible to most people may be impossible to access for students and others with disabilities. With the advancement of technology, the World Wide Web has gone from using a simple text-based format to using a robust designer format that includes widely used graphics, tables, photographs, and video and audio clips. Individuals with vision impairments must rely on screen readers or voice command software to read text aloud from Web pages, but such tools cannot read graphics or video clips. For a blind person, Web sites that rely on graphics can slow navigation to a crawl, and where the graphic provides vital information or is used to move around the screen (such as an arrow button), it may make navigation altogether impossible. People with hearing disabilities are also at a disadvantage because they cannot access audio clips unless they are provided access to a text version. Because schools must provide communication to those with disabilities that is *as effective as that provided to others*,[34] schools must use universal design principals to make their sites widely accessible. Universal design is the development of information systems that are flexible enough to accommodate the needs and preferences of the broadest range of users of computers and telecommunications equipment, regardless of age or disability.

HOW TO COMPLY

Fortunately, making a Web site universally accessible is not as difficult as it sounds. By using the following Disability Access Design Standard based on the city of San Jose, California,[35] schools should be able to make their sites universally accessible and comply with the ADA at the same time.

1) *Assess Your Web Site.* First, view your current Web site to see how accessible it is. Start by using a text-based Internet browser

34. U.S. Dept. of Education, Office of Civil Rights, Settlement Letter: Docket # 09-95-2205 (1996 Letter).

35. City of San Jose, World Wide Web Page, *Disability Access Design Standards (http://www.ci.san-jose.ca.us/oaacc/disacces.html).*

that has no provision for graphics or fancy fonts. This browser will enable you to move around your homepage and determine whether all your links are visible or not. If you select a link and the page reads only [image] [image] [image], you know you have a problem. The link is relying on graphics, and a blind visitor using voice command software will not be able to see (or rather hear) what the image is. Instead, the visitor will hear only the word "image" instead of a description of the image. Determine whether the page still makes sense without the graphics, tables or columns or whether providing a textual description would suffice as an alternative. Assess each trouble spot and use the following measures to address them.

2) *Provide an Access Instruction Page.* This page should provide instructions for access to your Web site for users with disabilities. It should be linked to your home page and ideally should provide an e-mail hyperlink for visitors to communicate problems with Web page accessibility.

3) *Provide Support for Text Browsers.* Support should be available directly on the page itself or should be provided by an alternative text page displaying the same information.

4) *Provide Alternative to PDF.* Documents posted in PDF (Portable Document Format) cannot be read by most screen readers, so a second version should be posted in an accessible format utilizing ASCII or text HTML.

5) *Use "Alt" Tags.* Attach an "Alt" tag to each graphic image and provide a short description of that image.

6) *Hyperlink Photographs with "D."* Link photographs on the page with a description button ("D") which can be used as a selectable hyperlink to a description of the photograph. Use a "Return" hyperlink at the end of the description to return the user back to the photograph.

7) *Hyperlink Audio and Video Clips with "CC."* Link audio and video clips with a closed-caption ("CC") link button that provides text transcriptions or descriptions.

8) *Use Descriptive Words as Links.* Avoid using words such as "click here" that do not convey information about the nature of the link.

9) *Provide Alternative Mechanisms for Access to Online Forms and for Downloading Software.* Since all browsers do not support all online forms (such as application forms) and screen readers may not be able to download software, provide phone numbers or e-mail addresses for users to access forms or assistance.

10) *Avoid Using Barriers.* Formats such as frames, tables and newspaper formats are not accessible by all browsers or screen readers and should be avoided wherever possible. Where they are necessary to the integrity of the page, provide proper descriptions of each.

AFFIRMATIVE DUTY

Courts have held that public entities have an "affirmative duty" under the ADA to evaluate their policies and procedures addressing services and programs for individuals with disabilities.[36] This affirmative duty means it is not enough to respond on an ad hoc basis to complaints or requests for accommodations, but rather policies must be formulated in advance, and the community of persons with disabilities must be consulted in the development of the policies.[37] A proactive approach is what is expected and

36. *Tyler v. City of Manhattan*, 857 F. Supp. 800 (D.Kans. 1994).

37. *Id.*

anticipated by the law. This means schools implementing new Web sites must ensure they are accessible from the beginning, and those with Web sites not yet in compliance must correct the problem as soon as possible. Furthermore, schools must not merely provide access to students and other individuals with disabilities, but must ensure the communication is equally effective.

ENSURING ACCESSIBILITY

While public policy and the ADA require the removal of barriers to effective communication, such compliance has other benefits as well. Ensuring universal design of Web sites makes the sites highly usable and available to everyone. For instance, many users lack "state of the art" technologies to access high-tech Web sites. Broad access is important because many visitors to the Web don't have the most updated browser software and cannot otherwise access a school's Web page. Additionally, many users get online access through devices such as PalmPilot or WebTV, or even through their telephones. Making the changes for people with disabilities ensures access for everyone. It involves giving high-tech users the tools and graphics necessary to keep the site fun and interesting, while allowing the low-tech or disabled user equally effective access to communication.

Physical security of technological equipment

Security has become a major concern as technology becomes more prevalent in schools. While the legal rules surrounding theft or damage to technological equipment are the same as for all other school property, administrators must take special precautions to protect their investment in such equipment. Policies must be instituted and followed to prevent theft, vandalism and misuse of equipment in both school and district level operations.

Equipment such as laptop computers and software is easily transportable and should be secured when not in use. To facilitate repair, newer computers are designed for easy removal of components (such as hard drives) that therefore are easily stolen unless properly secured. Computers themselves can have lock-down capabilities that should be utilized, and security systems can be used so an alarm will sound if wires are cut. Network hubs and other equipment to which few people need access should be kept in separate, lockable facilities. Areas not open to the public will require less attention than those widely accessible. Like all other aspects of the implementation of a technology plan, schools should assess their current and future security needs prior to the installation of technological equipment.

Internet Access and the E-rate

Access to the Internet is one of the most important aspects of a technology system. While computers and software provide valuable tools for learning, it is the Internet that opens the door to the unlimited world of online information. But as with technologies, schools must pay for access to the Internet. Now the federal government has enacted legislation to help schools in that endeavor.

In 1996, Congress passed the Telecommunications Act, P.L. 104-104, February 2, 1996, 110 Stat. 56, one of its broadest funding mechanisms ever. The purpose was to ensure that all Americans, particularly those living in low-income, rural and high-cost service areas, have access to affordable, quality telecommunications services.

The Telecommunications Act established the Universal Service Fund, commonly called the E-rate. The E-rate was created to provide the nation's elementary and secondary schools and libraries with deep discounts (20 percent to 90

percent) for services such as basic telephone service, advanced telecommunications services, Internet services and internal connections. Congress originally budgeted $2.2 billion in funding but has since scaled that figure back to $1.3 billion. The amount of discount awarded each school is tied to the schools' location (rural or urban) and economic need as determined by the level of eligibility in federal free and reduced-price school lunch programs. The Schools and Libraries Corporation (now the Schools and Libraries Division of the Universal Service Administrative Company) was created to administer and manage the application and funding process.

As part of the application process, schools applying for the discounts must submit a budget and a technology plan that meets certain criteria. The plan must include the school's strategy for providing professional development and for purchasing necessary hardware and software. Approval of plans may be granted by certain state education agencies. Additionally, schools must conduct a technology inventory and assessment of the telecommunications services it already uses as well as those it intends to purchase.

While the discounts available will be helpful to schools in obtaining telecommunications services, the E-rate does not provide for the cost of items such as hardware and software. In addition, the application procedure has been criticized by some as complex and cumbersome. Nevertheless, funds are available annually and eligible schools should take advantage of the E-rate to complement the many tools necessary to implement a technology system.

As with all legislation, the components of the E-rate are subject to change. For the most current information about the E-rate, visit the following Web sites:

E-rate Primer, developed by North Central Regional Technology in Education Consortium, *http://www.ncrtec.org/capacity/erate/*

E-rate Hotline, *http://www.eratehotline.org*

Schools and Libraries Division, *http://www.slcfund.org*

LearnNet, *http://www.fcc.gov/learnnet*

Education and Library Networks Coalition, *http://www.itc.org/edlinc*

U.S. Department of Education Technology Initiatives, *http://www.ed.gov/Technology*

Rodney A. Satterwhite and R. Craig Wood are partners and Calvin S. Spencer, Jr., is an associate with the Virginia law firm of McGuire Woods Battle & Boothe. Satterwhite is based in Richmond and practices in the area of labor and employment law, including technology issues in the workplace. Spencer and Wood are both based in Charlottesville. Spencer practices product liability law while Wood practices in education law, labor and employment law and other areas.

Resources

Helpful Web Sites

The World Wide Web Consortium Web Accessibility Initiative Resources, *http://w3.org/WAI*

Bobby, a Web site that will perform a free accessibility diagnostic and make suggestions, *http://www.cast.org/bobby*

Starling Access Services, a Web site that provides tools for webmasters, *http://www.igs.net/~starling/acc/index.htm*

More Than Screen Deep: Toward Every-Citizen Interfaces to the Nation's Information Infrastructure, Computer Science and Telecommunications Board, Commission on Physical Sciences, Mathematics, and Applications, National Research Council; National Academy Press 1997 Full text, *http://www.nap.edu/readingroom/books/screen*

Americans with Disabilities Act

Cynthia D. Waddell and Kevin Lee Thomason, "Is Your Site ADA-Compliant?" *The Internet Lawyer,* Nov. 1998, Issue 4.11

Cynthia D. Waddell, *Applying the ADA to the Internet: A Web Accessibility Standard, http://www.rit.edu/~easi/law/weblaw1.htm*

City of San Jose, World Wide Web Page, *Disability Access Design Standards, http://www.ci.san-jose.ca.us/oaacc/disacces.html*

Planning and Funding

Donn Ritchie & Karen Boyle, "Finding the Bucks for Technology," *Learning and Leading with Technology,* Vol. 26, No. 2, Oct. 1998 Southern Technology Council, 1997

Networking Schools. "For What Purpose?" *From Now On*, The Education Technology Journal, Vol 6 No. 9, June 1997

Doug Johnson, "The Less Simple Answer to Evaluating Technology's Impact," *The School Administrator,* Number 4, Vol. 55, April 1998

Gerald Bailey, *What Technology Leaders Need to Know*, Learning and Leading With Technology, Vol. 25, No. 1, Sept. 1997

Jamieson McKenzie, *Technology's Webs*, The School Administrator, Vol. 4, No. 55, April 1998

Dr. Chip Kimball & Peter H. R. Sibley, "Am I On the Mark? Technology Planning for the E-rate," *Learning and Leading With Technology,* Vole 25, No. 4, Dec/Jan. 1997-1998.

Gerald D. Bailey & David Pownell, *Technology Staff-Development and Support Programs*, Learning and Leading With Technology, Vol. 26, No. 3, Nov. 1998

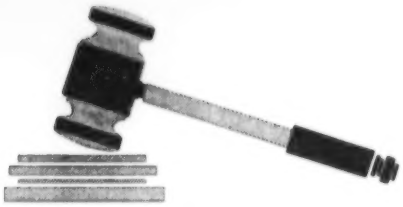
Mark Hawkes, *Funding a Technology Network in Your School*, Schools in the Middle, May/June, 1998

Reed Hundt, *Providing Opportunity for All Through the Telecommunications Revolution*, Bulletin, Vol. 80, No. 582, October, 1996

Notes

Chapter 3

Legal Considerations in Regulating Employee Use of School Technology



Bruce W. Smith*
Drummond Woodsum & MacMahon
Portland, Maine

Introduction

The time is fast arriving when there will be an Internet-connected computer on almost every public school teacher's desk. In many places that is already a reality. These in-class computers represent a giant leap forward, both quantitatively and qualitatively, in communications capability, information retrieval and information storage. The educational possibilities are boundless. But along with the daunting task of harnessing the power of computers to advance schools' core educational objectives comes the challenge of managing computer use by employees to prevent nonproductive, inappropriate and harmful uses of machines and networks.

This chapter addresses several issues relating to staff access to computers: personal use and privacy issues; collective bargaining; First Amendment concerns; rules governing staff computer use; and employee safety. The primary theme of the chapter is that by anticipating and understanding these issues, schools will best be able to manage the challenges they present.

* *A biographical sketch of the author is available at the end of this chapter.*

Personal use of school district computers

Despite falling prices, a personal computer is an expensive piece of equipment, far more costly than any other single tool provided by schools to their teachers. Most schools have determined, though, that the educational benefit justifies the investment. Research has shown that technology in the classroom can improve creativity, research skills and higher-level thinking skills.[1] It has also shown that students who use computer systems outperform those who don't by 25 percent to 41 percent.[2] Technology can have a big impact in the classroom.

Having endorsed significant spending on technology for students, teachers and other staff members, schools should also take reasonable measures to protect their investment. The temptation for staff members to make personal use of school computers, particularly those connected to

1. Donn Ritchie & Karen Boyle, "Finding the Bucks for Technology, Learning and Leading with Technology," Vol. 26, No. 2, Oct. 1998.

2. *Id.*

the Internet and/or school-wide networks, is probably irresistible. In certain cases, personal use is appropriate. Some school districts encourage employees to use district-owned technology as a means of familiarizing themselves with the function and range of features available for educational applications. Yet, when staff members use Internet-connected school computers for things like personal e-mail to other staff members, friends and family, it creates the risk that the district's e-mail accounts will be carrying inappropriate or even harmful materials.

Employees sometimes access the Internet's World Wide Web for personal reasons, creating the risk that they will view or download materials that are clearly inappropriate in any public school. They may download text or graphic files from the Internet or receive information and images via e-mail from other individuals. These files could carry viruses that are harmful to district operating systems. Employees may decide to add or change software, leading to the need for maintenance or repair. School districts should also be mindful that scanners and related technology allow employees to take outside images – such as inappropriate photos or documents – and introduce them into the school district's system, either as a pass-through on their way elsewhere or stored in the electronic memory.

"School districts have substantial discretion to prevent or regulate personal use of their computers. If they fail to exercise it ... they may find the district's computers being used in an unfettered fashion."

School districts have substantial discretion to prevent or regulate personal use of their computers. If they fail to exercise that discretion in a deliberate manner, however, they may find the district's computers, by default, used in an unfettered fashion by staff members for inappropriate personal use. Once that occurs, there may be legal and political hurdles that make it more difficult to reassert control over the district's computer systems. [See *Rules & Policies for Employee Use of School Computers* later in this chapter for a review of issues on how to regulate employee use.]

Privacy

The common strand underlying the various legal theories concerning employee computer privacy is that the employee must have a "reasonable expectation of privacy" in the material in order to assert a successful legal challenge. Employees' expectations regarding privacy, or the lack of it, are largely determined by the employer's policies, rules and practices concerning use of the school computer system. By developing and distributing those rules, the school is able to define the zone of privacy, if any, that staff members have in their use of the system. Even where an employee has a reasonable expectation of privacy, the employer will not be found to have violated the employee's privacy right if the employer acted reasonably under all the circumstances.

Should Employee Acceptable Use Policies or rules afford staff members any privacy interests in e-mail or stored files? As a practical matter, school administrators probably have no desire to review all e-mail or to scour computer hard drives on a regular basis. In order to retain the maximum degree of legal authority to search computer files and networks, however, schools should consider establishing very clear rules stating that school officials can and will search data or e-mail stored on all school-owned computers at any time for any reason, and that staff members have no right of privacy in any such data. Such rules come in handy in a variety of legal circumstances.

In one case, for example, a teacher alleged that another teacher was sexually harassing her, but the alleged harasser denied the charge and there were no witnesses. A search of the alleged harasser's computer produced copies of harassing e-mails that the victim had not saved. In another case, school officials believed a school custodian was accessing pornographic Web sites while on duty, but no one had ever observed him doing it. A search of the log on his Web browser produced ample evidence. The superintendent (averting her eyes) printed copies of a number of the offensive Web sites. When the employee's attorney was shown this graphic and irrefutable evidence, the employee promptly resigned.

Fourth Amendment

As employees of governmental entities, school staff members have a right under the Fourth Amendment to the U.S. Constitution to be free from unreasonable searches and seizures. The United States Supreme Court ruled in the case of *O'Connor v. Ortega*[3] that the Fourth Amendment applies only when a public employee has "an expectation of privacy that society is prepared to consider reasonable." Whether such an expectation exists depends upon the circumstances, including the employer's policies and practices. That said, school boards can purposefully act to erase an expectation of privacy by passing a comprehensive policy – in essence putting employees on notice that personal privacy doesn't apply for school-owned computers. That becomes important because if the employee has a reasonable expectation of privacy, the public employer is restricted and may conduct a work search only if "reasonable under all the circumstances."

It is likely a court would apply this rule to searches of employee computer files and electronic mail. If the employee has a reasonable expectation of privacy in those files, the employer must have a reasonable basis to review them in order to comply with the Fourth Amendment.

Electronic Communications Privacy Act

The federal Electronic Communications Privacy Act[4] (ECPA) also protects the privacy of electronic communications, including electronic mail. The ECPA contains an exception for the provider of the electronic communications service, which generally is viewed as including employers who provide a computer system or portable laptop for use by employees at work or on work-related tasks.[5] In addition, the ECPA does not apply when an individual has consented to the monitoring, and consent may be implied from the circumstances.

Generally speaking, then, the ECPA is not likely to present a significant obstacle to school district monitoring of employee e-mail communications. The best way to ensure the law is not violated, however, is to have in place a policy notifying employees that their e-mail is not private and that it will be monitored, and to disseminate that policy to all employees.

Common law privacy

Another potential legal basis for a right to privacy in computer files and e-mail is the "common law" right to privacy.[6] An employee whose e-mail has been reviewed by the employer may file a common law suit in court for invasion of privacy. The tort of invasion of privacy requires the intrusion into privacy be

3. 480 U.S. 709 (1987).

4. Pub. L. No. 99-508, 100 Stat. 1848, also 18 USC Section 2510-2522.

5. Kevin J. Baum, *E-Mail in the Workplace and the Right of Privacy*, 42 Vill. L. Rev. 1011, 1024 (May 1997).

"highly offensive to a reasonable person."[7] The employee must have a reasonable expectation of privacy in the material reviewed in order to prevail on such a claim. In two different court cases where an employee asserted that the employer's interception of his e-mail was a violation of his common law right to privacy, the courts ruled against the employee. In the first case, the employee had signed a waiver acknowledging that e-mail use was limited to "company business."[8] In the second case, the employer had sent the e-mail to his supervisor.[9]

Computers are designed to retain data of all kinds, resulting in the preservation of a great deal of information that simply would not have been available in the past. Documents that would once have been discarded now often end up saved unintentionally in computer files on individual hard drives or on network servers. Communications that would once have occurred orally by telephone or face-to-face are now memorialized in electronic mail. Research that might have left no tangible record in the past is now available for the asking because the session is preserved on Web browser logs. The availability of all this information may prove to be a useful tool to schools when allegations of employee misconduct are investigated. While school officials should use restraint and good judgment in conducting searches of employees' digital information, they are well-advised to retain the authority to conduct such searches by notifying employees they have no privacy rights therein.

6. The common law is the body of widely accepted legal principles developed over time by judges deciding court cases, as distinguished from the Constitution, statutes and regulations.

7. Restatement (Second) of Torts, Section 625B.

8. *Bourke v. Nissan Motor Corp.*, Cal. Super. Ct. No. YC003979 (Cal.App. 1991).

9. *Smyth v. Pillsbury Co.*, 914 F.Supp. 97 (E.D.Pa. 1996).

First Amendment issues

Most of the legal issues involving computers in schools stem from the use of computers for communications such as e-mail, Web-browsing and chat. Wherever there is a communication of ideas, the First Amendment right of free speech is likely to apply. The Internet as a whole has been deemed by the Supreme Court of the United States to be a forum where the highest degree of First Amendment protection applies. In the landmark case of *Reno v. ACLU*, the Court said, "[A]ny person with a phone line can become a town crier with a voice that resonates farther than it could from any soapbox."[10] If the Internet is a constitutionally protected marketplace of ideas – an electronic town square – can schools restrict expression by teachers that is carried over the Internet?

Teacher speech Just because government cannot restrict freedom of speech on the Internet does not mean schools cannot restrict expression by school employees on the school's computer systems. School employees retain the right under the First Amendment to speak freely on matters of public concern, but the school may restrict the speech of an employee when the employee is acting strictly out of personal interest.[11] A matter of public concern would include, for example, an issue about the quality of teaching, administration of the school district and even matters of educational philosophy. By contrast, a private concern might be a person griping about her or his own salary or the discipline received in response to a specific incident. Thus, the school may prohibit or punish inappropriate employee communications on the school's computer system when the speech is not on a matter of public concern. Additionally, schools have the same right to regulate speech when teachers are implementing the board-approved

10. 117 S. Ct. 2329 (1997)

11. *Connick v. Myers*, 461 U.S. 138 (1983); *Pickering v. Board of Education*, 391 U.S. 563 (1968).

curriculum or otherwise acting in their official capacity.

The more difficult question involves the regulation of speech on a matter of public concern that is protected by the First Amendment. Whether employees will have enforceable free speech rights on the school's computer communication systems will depend primarily on whether the school has permitted the system to function as an open or limited open forum for expression of ideas by teachers. As an example, consider a case where teachers become active in local school board elections, with the goal of ousting the current members of the board and electing new members. Teachers begin sending mass e-mails to other staff and even to many parents whose e-mail addresses they have collected. The mass e-mail provokes many e-mail responses and a wide-ranging e-mail discussion of the school board's performance. If the school has no clear policy on employee use of the e-mail system, and it has been used extensively by teachers for expression of views on political, educational and other issues, the authority of the school administration to restrict this political activity will be in doubt. The courts frown upon content-based restrictions on speech. By failing to establish rules for use of the school computer system, the school has permitted an open forum to exist, and it will be hard-pressed to ban discussion of particular subjects or views – no matter how distasteful to district officials.

Can a district halt electronic politics without violating free speech rights?

If the school has a clear policy stating that electronic communication systems are to be used by employees only for the performance of their jobs, then a district can direct the staff to discontinue any political activity on the system.

If, on the other hand, the school has a very clear policy stating that the electronic communications systems are to be used by employees only for the performance of their jobs, all other uses are prohibited, and the system is not a forum for the expression of personal opinions on any subject, then the administration will be in a much stronger position to direct the staff to discontinue the political activity on the system. The action will not be based on the point of view expressed or the particular subject matter of the communication, but solely on the fact it is not a work-related use of the system.

Restrictions on Teacher Internet Access

Just as the school may restrict communication by school staff to work-related purposes, it may also restrict World Wide Web research to work-related purposes. A February 1999 decision by the 4th U.S. Circuit Court of Appeals in Virginia says schools may restrict the scope and nature of a teacher's Web research (whether elementary-secondary or higher education) and academic freedom concerns are overridden. In *Urofsky v. Gilmore*[12] the 4th Circuit Court ruled that a statute barring all state employees from using state computers to display on their screen, download, print or store files having "sexually explicit content" does not violate the Constitution's First Amendment freedom of speech.

The plaintiffs in the case were professors at state colleges and universities who claimed the law unconstitutionally restricted access to material they needed for academic pursuits. The court reasoned that the professors are state employees and their right to receive material in that role is limited. The opinion asserts that "…the state, as an employer, undoubtedly possesses greater

12. No. 98-1481 (4th Cir., Feb. 10, 1999). *Formerly Urofsky v. Allen*, where U.S. District Court for the Eastern District of Virginia on Feb. 26, 1998 sided with the professors.

authority to restrict the speech of its employees than it has as a sovereign to restrict the speech of the citizenry as a whole." Since the need for Web access involves an employee (university professor) in his or her capacity at work, the speech cannot possibly be considered "a matter of public concern" and the extra protections that usually go along with it are withheld.

The 4th Circuit noted that the act allows the university professors to pursue any research they please if they get prior permission. The law contains an exception for a "bona fide, agency-approved research project or other agency-approved undertaking." Interestingly, despite the more traditional latitude given to academic freedom in higher education, the court used a public school case as controlling this situation. It cited the 1998 case of *Boring v. Buncombe County Board of Educ.*[13] In *Boring*, the full panel of 4th Circuit judges upheld the dismissal of a drama teacher who selected a play that included teen pregnancy and lesbianism for her high school students to perform. The judges based their opinion on the fact that the school district has ultimate control over matters dealing with curriculum and the teacher was operating in her professional capacity. Drawing a parallel line, the court said the professors in *Urofsky* were similarly asserting a right to control academic content and were also operating in their official capacity. They restated that the power to do those things, as established in *Boring v. Buncombe*, rests with the state. Last, the court also pointed out that professors in their personal capacity at home had every right to call up any Web site of their choosing.

In a similar Oklahoma case, a district court judge upheld the authority of Oklahoma University to block certain news groups accessed through the university news server. Citing the First Amendment, a group of professors in *Loving v. Boren*[14] challenged the practice of separate news servers for employees and students. The employee server allowed unlimited access for academic research while the student server prohibited access to information the university considered obscene.

In addition to curricular control, the public schools in general have a greater obligation to protect minor children from access to inappropriate material. If teachers download such material, the risk is increased that children will be exposed to it. Therefore, it makes sense to apply the same rules the district selects to restrict student access to inappropriate materials to teachers and other employees as well.

Rules and policies for employee use of school computers

Schools should establish a clear set of separate rules concerning staff use of their school-provided computers and the school's network and Internet connection. Such rules will reduce misuse of the systems and will provide the foundation for discipline should misuse occur.

Schools have taken a variety of approaches in regulating staff/employee use of computers and the Internet. In the rush to implement Acceptable Use Policies for students, some schools have neglected to adopt any policies concerning employee use of computers. Others have incorporated staff into a general Acceptable Use Policy.

Clearly, rules for employee use of school computers should be promulgated and disseminated. In this writer's view, it makes more sense to have a separate policy for employees, who are adults and who are likely to be held to different standards than students. A policy for employees might address the following issues:

13. *Boring v. Buncombe County Bd. Of Educ.*, 136 F.3d 364 (4th Cir.) *(en banc), cert.* Denied 119 S. Ct. 47 (1998).

14. *Loving v. Boren*, 956 F.Supp. 953 (W.D. Okl. 1997)

Personal Use As the most restrictive approach to personal use, a school district may mandate that district computers, networks and Internet connection shall be used only for purposes related to the schools and the performance of the employees' jobs, and no personal use of any kind is permitted. This would prohibit personal e-mail, creation of personal word processing documents, personal Web-surfing and all other personal activities. It would also prevent all kinds of solicitation – political, religious, commercial, non-profit – without regard to the content of the solicitation.

The advantage of this approach is that it sets a clear, bright-line rule that all employees should understand. If obeyed, the rule will protect the school district's computers from inappropriate uses. Enforcement will be very difficult, and employees are likely to violate the rule on a regular basis, but the rule will provide the school the authority to act decisively when it becomes aware of violations.

An alternative approach that recognizes and permits some personal use might be expressed in the following statement:

> *School computers, networks and Internet access are provided to support the educational mission of the school. They are to be used primarily for school-related purposes. Incidental personal use of school computers must not interfere with the employee's job performance, must not violate any of the rules contained in this policy or the Student Acceptable Use Policy, and must not damage the school's hardware, software or computer communications systems.*

Copyright The policy should contain a rule against illegal publication or copying of copyrighted material, and a statement that employees will be held personally liable for any of their own actions that violate copyright laws. [See Chapter 4: *Copyright in the School Domain* for more information on this topic.]

Confidentiality Employees should be directed not to transmit confidential information concerning students or others over systems not designated for that use, and to use care to protect against negligent disclosure of such information.[15] Because of concerns about confidentiality in electronic communications, some schools construct or purchase special secure systems that safeguard information.

Privacy As discussed above, the policy should provide that all data stored or transmitted on school computers can and will be monitored, and that employees have no right to privacy with regard to such data.

Harassment The employee policy should remind employees that school policies against sexual harassment and other forms of discriminatory harassment apply equally to communication on school computer systems.

Misuse of networks, hardware or software The policy may provide that damage caused by intentional misuse of equipment will be charged to the user.

---

15. The federal Family Educational Rights and Privacy Act restricts disclosure of personally identifiable information from a student's "educational records." An e-mail message itself may well constitute an "education record" which should be protected under the law. When a staff member communicates with another staff member concerning a student and for legitimate educational purposes, that kind of information-sharing is not prohibited by FERPA. Disclosures about students to staff members who have no need for the information or especially to outside persons, could violate FERPA.

    In addition, employee information transmitted electronically should also be guarded against inappropriate disclosures that may violate state employee privacy laws or common law rights of privacy.

Safeguard accounts and passwords Employees should be reminded they are responsible for safeguarding their own passwords, and they will be held accountable for the consequences of intentional or negligent disclosure of this information.

Illegal uses Local policies should attempt to identify categories of illegal uses to put employees on notice.

Advertising School employees are often involved in outside businesses, and they may find it tempting to advertise or solicit on the school's e-mail system for such products as Amway, Avon or Tupperware. Such advertising can unnecessarily clutter the school's e-mail system and will probably be unwelcome to most recipients. The best way to prevent this is for the school district to adopt a policy that prohibits advertising and solicitation on school computers. The policy should be broad enough to prohibit an employee from sending messages from a home or other outside computer to school district e-mail users.

Fundraising, non-profit or charitable solicitation Another common use of e-mail is to solicit or announce fundraising events for non-profit organizations. Schools may decide they will allow such use, perhaps with prior approval, or they will forbid it. Districts should be careful, however, if they permit fundraising activity to take place that they do not discriminate and bar any speakers based on the message. Whether the use is permitted or not, the issue should be addressed in the employee use policy.

Representing personal views as those of the school district Any e-mail sent from the school computer is likely to contain a return address identifying the school district. Thus, sending an e-mail from the school is analogous to an employee using school letterhead.

Accordingly, employees should be put on notice to be careful not to have their own statements mistakenly attributed to the district.

Downloading or loading software or applications without permission from the administrator There is an enormous quantity and variety of free software available on the Internet. In addition to viruses that could infect the school's systems, the cumulative effect of widespread downloading on the school's computers, in terms of degradation of performance and additional maintenance, can be significant. School districts can prohibit use of outside software, or place restrictions on it, such as by requiring pre-approval from the technology coordinator or system administrator.

The role of the technology coordinator/system administrator

In many schools, the technology coordinator is more likely than any other person to discover violations of use policies. It is important that the duties of the technology coordinator match coherently with the Acceptable Use Policy. Even if this person is not in a position to handle disciplinary matters, the coordinator may play an important role in reporting and investigating violations. The coordinator may be required to report all violations of the policy to a particular administrator, to preserve evidence of the violation in digital form and/or hard copy, and to assist the administrator in further investigation involving the school computer systems.

The technology coordinator should also be given clear direction concerning confidentiality. This person will necessarily have access to information – such as student information protected by the Family Educational Rights & Privacy Act, confidential employee information, and confidential administrative communications – that he or she should not share with others. By

clearly defining the individual's duties in a job description or written memorandum, the school can help to prevent mistakes resulting from lack of awareness of confidentiality concerns.

Collective bargaining

The Duty to Bargain Most states permit school employees to bargain collectively with school boards. In general, bargaining laws require employers to negotiate about wages, hours and working conditions. The precise scope of the duty to bargain and the exceptions to this duty, however, vary from state to state. Under general principles of collective bargaining, it is likely that certain aspects of employee use of school computers will be mandatory subjects of bargaining.

Unions may demand to bargain on such issues as employee privacy rights, use of e-mail for disciplinary purposes, personal use of the school's computer systems, and liability for damage to the systems. Because state laws on collective bargaining vary and because these issues are new to collective bargaining, it is not possible to generalize about whether school boards have a duty to negotiate concerning specific issues. School board negotiators should not be too quick to concede the negotiability of these issues, however, and should consult with their attorneys or bargaining consultants concerning theories that would support a refusal to bargain. Once provisions securing employee and union rights to school technology are ensconced in contracts, they will become very difficult to remove.

Union Use of Computer Systems Teacher collective bargaining agreements often contain provisions allowing the union and teachers to have access to school mailboxes, interoffice mail delivery, bulletin boards and telephones. Unions often are permitted use of school equipment, particularly copiers, for union business. Unions are increasingly seeking access to the power of computers and computer communications, and they can be expected to attempt to bargain for access to and use of the school's computer systems.

E-mail can provide unions with instant access to all members. Through the use of mass e-mail messages, union leaders can quickly galvanize their entire membership with regard to particular issues. E-mail also can improve unions' communications with their professional representatives.

School board negotiators should consider all the implications before agreeing to union use of a school's computer systems. Permitting union use of those systems will increase system traffic, thereby increasing the risk of network problems related to such traffic. Staff members receiving union-related e-mails at work can be distracted or even disrupted. In addition, allowing unions unfettered use of school communications systems provides them a very powerful medium that may be used in a manner adverse to the school board's interests and goals. Because the cost of allowing union use of existing systems may be negligible, school board negotiators may be quick to agree to it. Such access should have great value to the union, however, and at the very least school boards should expect to get something of value in return for agreeing to it.

If collective bargaining does not govern board-union relations, districts should seek to clearly define whether union use of e-mail is permitted.

Employers must also be very careful about prohibiting or penalizing use of the school e-mail for union organizing or other concerted activities. The National Labor Relations Board has ruled that an employer may not ban union access to an e-mail system where employees were allowed to use the system for other personal purposes.[13] Although federal labor law does not apply to local public schools, state public employee bargaining laws are often modeled on the federal law and interpreted in a similar way. Unless the issue is fully covered by collective bargaining agreements, school employers should give careful thought to how they wish to address

Considerations in granting labor union access to school district computers

1. School boards should ponder all the implications of access before granting consent.
2. Unions could use this powerful communications medium to defy the school board's interests.
3. Because of the small financial cost of allowing unions to use existing systems, school board negotiators may be prematurely quick to agree to it.
4. Such access has great value to unions and at the very least school boards should expect to get something of value in return.
5. Without a collective bargaining agreement, school boards may choose to clearly prohibit or penalize use of the school e-mail system for union organizing or other activities.

union activity in employee e-mail policies, and are well advised to consult their labor relations attorney when doing so.[16]

Technology Training for Teachers The addition of computer technologies to classrooms and libraries will be of little use if teachers do not know how to use them effectively in the educational program. As with any other new educational program or tool, effective use requires training, and schools must struggle with ways to provide efficient training to teachers. Contractual restrictions on training time may impair a district's efforts to provide adequate training. Restrictions on the number of work days, the length of days and the number of after-school sessions and requirements for outside course work all may come into play when schools seek to train teachers on making effective use of technology.

Depending upon the applicable bargaining law and the existing contract, school boards may have to bargain with teachers' unions for adequate training time and/or for additional compensation for that time. In general, however, the collective bargaining implications of computer training are the same as those that apply to other mandatory teacher training. There will be pressure from unions either to provide release time or additional compensation for such additional training requirements.

Working safely with computers

It is now generally accepted that the use of computers and video display terminals can cause or aggravate certain health problems. Complaints include excessive fatigue, eye strain and irritation, blurred vision, headaches, stress, and neck, back, arm and muscle pain. Some have also raised concerns about exposure to electromagnetic fields radiating from computers.

Frequent users are more likely to suffer from these symptoms than those who use computers only for brief periods daily, but it is reasonable to assume that as the rate of computer use by staff members increases overall, so will the rate of symptoms attributed to that use. When staff members suffer such symptoms, they are more likely to be absent from work and to file workers' compensation claims for medical expenses and lost time. Proper training, supervision and furnishings for computer users can, however, help to prevent injuries that result from improper use of computers.

16. A useful discussion of this issue can be found at: Kim M. Tarn, "Union Activity by e-mail: Another Topic for the Employee Handbook," http://www.lclark.edu/~loren/cyberlaw97/tran/Union%20Email.html (fall 1997).

The health risks

According to the Occupational Safety and Health Administration (OSHA) of the U.S. Department of Labor, the primary areas of health concern are as follows:[17]

- **Visual Problems**

Eye strain and irritation are among the most common complaints by people operating computers. These symptoms may be caused by improper lighting, glare from the screen, position of the screen, or materials that are difficult to read.

- **Fatigue and Musculoskeletal Problems**

When computer users maintain a fixed posture over long periods of time, they may suffer muscle fatigue and, after awhile, muscle pain and injury. Users are also at risk for various musculoskeletal disorders such as carpal tunnel syndrome and tendinitis. These problems can cause chronic pain or even permanent disability.

Such problems can be especially acute for students at school because of poor posture used while working at a computer. According to a study to be published in the May 1999 edition of *Computers in the Schools*, "some elementary school computers are set up without accommodation for healthy typing postures, and that could put children at risk of developing the painful repetitive stress injuries that have affected office workers in recent years."

The study, conducted by Cornell University researcher Shawn Oates, is based on the observations of 95 researchers who watched elementary school children from 11 schools as they worked at computers in classrooms and computer labs. The study found "striking misfits" when comparing the size of the children and the computer workstations they used.

17. "Working Safely with Video Display Terminals" OSHA Publication No. 3092 (1997).

- **Radiation**

Some have expressed concern that radiation emissions from computers could pose a health risk, particularly for pregnant women. According to OSHA, there is no conclusive evidence that the low levels of radiation emitted from computers pose a health risk to operators. The issue is still being researched and studied.

Prevention of computer-related injuries

Schools have a significant interest in preventing injuries and adverse symptoms of computer use in order to keep their employees healthy, to prevent absenteeism and job modifications necessitated by such conditions, and to prevent workers' compensation claims that will increase insurance rates. Certainly, clerical workers and others using keyboards and monitors for a large portion of the work day are most at risk, but other staff members such as teachers who use computers at work at an increasing rate also can benefit from preventive measures.

The literature on injuries to operators of video display terminals indicates that most injuries can be prevented or minimized through training and proper use of the equipment. The design of the work station, including keyboard height and angle, monitor height, lighting and seating, can all affect the health of the user. In addition, the behavior of the user will have a direct effect on the risk of symptoms, including posture, sitting position, the introduction of variety into work routines and the taking of regular breaks.

Because environmental and behavioral factors are so pivotal in preventing injuries resulting from computer use, schools can do a lot to reduce the incidence of symptoms by setting all work stations properly, training all users and supervising users to comply with safety rules. Training can be provided in a variety of ways. Publications are available to instruct employers

and employees on proper design and use of computer work stations. One such publication is "Working Safely with Video Display Terminals," OSHA 3092 (1997 Revised).

On-site training usually is even more effective. Some workers' compensation providers give free training to employees. Insurance companies may even reduce policy rates if such training is provided. The most effective method is to have the trainer visit and observe the work station of each user. Larger school districts may train one of their own employees to provide such training in-house, including follow-up visits with computer users to ensure they are adhering to good safety practices. In addition, workplace health consultants may be hired at a fee to provide staff training.

While the training is most important for heavy computer users, all staff members who use computers in their work should receive some training on safe practices. Teachers in particular tend to set up their personal work spaces in their classrooms in unique ways. The school may set parameters that prevent any computer set-ups that increase the risk of adverse physical symptoms.

One significant benefit of implementing and maintaining a program of computer safety training is the financial savings that will result from fewer absences and workers' compensation claims. The costs of computer safety may include training, additional furniture and lighting changes. While any significant expenditure will, and should, prompt a cost-benefit analysis before a purchasing decision is made, the school's investment in safety is likely to pay off in the long run both for individuals and for the budget.

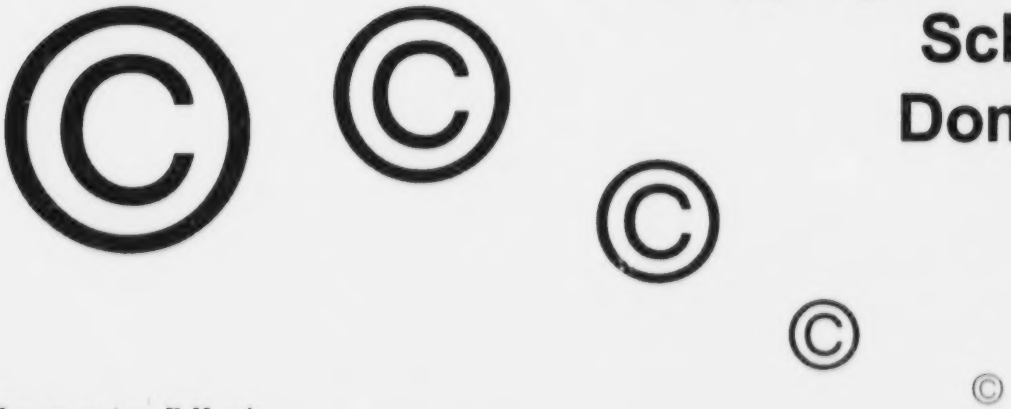
Conclusion

Staff access to networked and Internet-connected personal computers poses a number of new challenges and wondrous opportunities for public schools. The promise of instant information access is exciting and opens brand new chances to achieve educational meaning for each child. By planning and developing appropriate rules and policies, schools should be able to meet and adjust to those challenges, and thereby to help technology make learning more productive.

Bruce W. Smith is a partner with the law firm of Drummond Woodsum & MacMahon in Portland, Maine. He has represented school districts for more than 12 years and is co-author of the book* Maine School Law. *Smith has developed a special interest in legal issues concerning electronic communications in schools and is a frequent speaker and writer on school law topics. He is an instructor for the University of Southern Maine Law School and a director of the National School Boards Association's Council of School Attorneys.

Chapter 4

Copyright in the School Domain



Margaret-Ann F. Howie
Legal Counsel to the Superintendent
Baltimore County, Maryland, Public Schools

Introduction

As the Information Superhighway grows even more well-traveled, school decision makers will need to acquire a basic understanding of copyright law and how it relates to materials that are copied, recorded or transmitted via electronic media. This chapter presents an overview of copyright law for the non-legal policymaker and explains the fundamental principles. It will also address issues pertaining specifically to public schools, such as student and teacher-created work, fair use and the use of digital technology in the classroom.

Many issues remain unresolved in trying to determine educational fair use in the Information age. Even the 1998 Digital Copyright Millennium Act (H.R. 2281, Public Law 105-304, 112 Stat. 2827), which sought to address some of these issues as an amendment to the Copyright Act, left lingering questions. Also, as technology changes, new challenges will arise and new rules must be developed to maintain the delicate balance between the rights of the copyright holder and the need for society to use some of its best creations for educational purposes.

GENERAL PRINCIPLES OF COPYRIGHT

All copyright law is federal and is based upon the United States Constitution. Article I, Section 8, Clause 8 states that:

"Congress shall have power . . . to promote the progress of science and useful arts by securing for limited times to authors and inventors the exclusive right to their respective writings and discoveries."

What is copyright?

Copyright protects the ability of an author to be financially rewarded for the fruits of her creativity and presentation of ideas. It also provides a continuing incentive for U.S. citizens

* *A biographical sketch of the author is available at the end of this chapter.*

Example 1. What can be copyrighted

Zora Neale is a library media specialist at Harlem High School in the Renaissance School District. Zora has devised a software program that can be used to assist students to improve their reading comprehension skills.

Answer: Zora can copyright her software program. Under the law, the software program is a "literary work." Under the Copyright Act, Zora's software program can receive copyright protection. It can be "perceived" and "reproduced" and is embodied in a tangible form.

Example 2. What can be copyrighted

Suppose now Zora performs a demonstration lesson for members of the administration and school board.

Answer: Unlike the software program, the demonstration lesson cannot be "fixed." (It is over after she has taught it.) Copyright protection begins from the moment an idea has been "fixed" in a "tangible medium." Zora would not be able to receive copyright protection for the demonstration lesson she has performed. Note, however, that a recording of Zora's demonstration lesson would receive protection.

to conceive artistic, literary, musical and dramatic works – from which all of society benefits.

Copyright is a powerful legal tool, giving the author exclusive right to distribute, modify, perform, copy, display or otherwise decide the fate of his work. The author can give other people permission to use the work, called a license, and is usually compensated accordingly.

Because copyright is a form of property – sometimes called intellectual property – it can be sold, transferred or licensed, just like land or merchandise. For example, many copyright owners license to school districts the right to perform plays or musicals.

What can be copyrighted?

Copyright law extends to original works of authorship, fixed at any tangible medium of expression now known or later developed, from which they can be perceived, reproduced or otherwise communicated, either directly or with the aid of a machine or device.

Ideas cannot be copyrighted.[1] Rather, copyright protects the *manner* in which an idea has been expressed, which is embodied in a "work of authorship."

The law places works of authorship into the following categories:[2]

- literary works
- musical works, including accompanying words
- dramatic works, including accompanying music
- pantomimes and choreographic works
- pictorial, graphic and sculptural works
- motion pictures and other audio visual works
- sound recordings
- architectural works

1. 17 U.S.C. 102(b) "In no case does copyright protection for an original work of authorship extend to any idea, procedure, process, system, method of operation, concept, principle, or discovery, regardless of the form in which it is explained, illustrated or embodied in such work."

2. 17 U.S.C. 102

THE PURPOSE OF COPYRIGHT

The purpose of copyright law is to benefit the public good through the twin goals of *promotion* of public interest and *protection* of private rights. That is, the public is able to benefit from the fruits of the creative process through the protection granted to individual authors. Because the creator has the right to control her product, her economic interests are protected from unfair exploitation.

School officials should be aware that if a savvy teacher devises a software program that helps students, the program qualifies for copyright protection as a "literary" work. It is a work, fixed in a tangible medium that can be perceived and reproduced. Whether the school district or the teacher owns the copyright will depend on the circumstances [See page 59: *Copyright and employment: Who is the owner?*].

It is not necessary to place any copyright notice[3] on a document or to register a work with the Copyright Office in order to receive any of the rights conferred by the statute.[4] Therefore, neither students nor staff members should assume a work lacks copyright protection because of the failure to register it with the Copyright Office. Similarly, there is no requirement to place a notice of copyright on an item in order to confer an owner's exclusive rights. Nonetheless, it is a good practice to place a copyright symbol (©) on creations. This provides explicit notice to the world of the copyright owner's control. In some cases, it may give the potential copier pause before reproducing something and remind him of his obligations under the law to obtain permission.

Certain rights can only be enforced if a work is registered. Under 17 U.S.C. Section 412, a copyright owner cannot receive money damages or attorney fees for unpublished work or certain other works unless registration requirements have been met.

FAIR USE OF COPYRIGHTED MATERIALS

Perhaps one of the most misunderstood, and consequently abused, provisions of the Copyright Act is the fair use principle. The idea is to give learning institutions and certain others an opportunity to use copyrighted works to advance knowledge. The Copyright Act provides that the fair use of a copyrighted work for purposes of teaching, scholarship or research is not an infringement of copyright. In short, fair use provides cost-free access to the author's work even *during* the term of copyright protection. Fair use attempts to balance the author's right to control against the public's need for access to a copyrighted work.

There are four basic factors that courts use to determine fair use:

(1) Purpose – Whether the usage is for commercial gain for non-profit or educational purpose. The more commercial in nature an act is, the less likely it is to fit under the umbrella of fair use.

(2) Nature – The question centers on whether the work is fact or fiction. A fictionalized portrayal is more likely to be deemed fair use than one close to or derived from an actual fact.

(3) Substantiality – The court will examine how much of a full work was used. The larger the portion used, the more likely the user will be found in violation.

(4) Market Effect – The court will examine whether a copying incident has significantly impaired the ability of the author to profit from the work. The question is: based on what you did, what is the impact on the potential market for the work?

3. The standard notice of copyright consists of the symbol ©, or the word "Copyright," or the abbreviation "Copr.;" the year of the first publication of the work; and the name of the owner of the copyright. 17 U.S.C. 401.

4. 17 U.S.C. 102(a).

EXCLUSIVE RIGHTS

Copyright law gives to the owner of a creative work the exclusive right to:

- Reproduce the copyrighted work in copies or phonographic records;
- Create derivative works based upon the copyrighted work (e.g., from books to movies; to musicals from books);
- Distribute copies of the copyrighted work to the public by sale, rental, lease or lending;
- Perform publicly any literary, musical, dramatic or choreographic work;
- Display publicly any sculpture, motion picture, picture, graphic work or pantomime.[1]

1. 17 U.S.C. 106

The application of the fair use standards is far from an exact science. Congress has called fair use an "equitable rule of reason" with "no generally applicable definition . . . possible."[5] Therefore, it is impossible to state with certainty when a use will be considered copyright infringement or fair use. Because Congress declined to design a blanket exception for classroom use of copyrighted works, teachers, students and school administrators are, essentially, held to the same legal standard as commercial users.[6]

Guidelines for classroom copying of books and periodicals

Please note that the *Guidelines for Classroom Copying in Not-for-Profit Educational Institutions* are explicitly limited to books and periodicals, and do not encompass other types of copyrighted works, including computer programs.

GUIDELINES

Single Copying for Teachers

A single copy may be made of any of the following by or for a teacher for research or use in teaching or preparation to teach a class:

A. A chapter from a book;
B. An article from a periodical or newspaper;
C. A short story, short essay, or short poem, whether or not from a collective work;
D. A chart, graph, diagram, drawing, cartoon or picture from a book, periodical, or newspaper.

Agreed MARCH 19, 1976.
Ad Hoc Committee on Copyright Law Revision

5. H.Rep.94-1476, at 65. Courts, too, have stated their inability to apply the fair use standards mechanically: "The fair use doctrine permits courts to avoid rigid application of the copyright statute when, on occasion, it would stifle the very creativity which that law is designed to foster." *Stewart v. Abend*, 495 U.S. 207, 236 (1990). *See also Campbell v. Acuff-Rose Music*, 114 S.Ct. 1164 (1994)(parody might be within the bounds of fair use)

6. *See Marcus v. Rowley*, 695 F. 2d 1171 (9th Cir. 1983) (public school teacher sued for use of copyrighted material in her home economics class failed to prove that her copying was within the bounds of fair use)

During discussions relating to the 1976 amendments of the Copyright Act, the House Committee concluded that concrete educational guidelines as "a reasonable interpretation of the minimum standards of fair use" were necessary. The Committee convened a group of education users and copyright holders to draft a set of guidelines to be followed by education institutions. They include: *Guidelines for Classroom Copying in Not for Profit Educational Institutions*, *Guidelines for the Educational Uses of Music* and the *Guidelines for Off-Air Broadcasting*. [See "Resources" at the end of this chapter for Web site where these are available.]

How Your School District Can Benefit from the Fair Use Guidelines It is important to note that the guidelines are not a part of the copyright law. No school district is required to follow them. However, the guidelines provide a quantifiable standard for applying copyright law to everyday classroom situations and can be used as proof of a school district's good faith effort to follow the law. The guidelines are considered the minimum, rather than the maximum, of fair use. Therefore, any school district that followed them would be within a safe harbor.

School districts should consider distributing the guidelines to staff members and to students at the beginning of each school year. Many school boards have incorporated the guidelines into their policy statements.

Copyright Infringement An individual who violates an owner's copyright is subject to both civil and criminal penalties under the Copyright Act. Copyright owners can sue for statutory or actual (e.g., lost profits) damages in an infringement action. Additionally, they may ask for attorneys' fees and injunctive relief to bar further infringement. Because contributory infringement has been recognized by the courts, school districts can be held liable for the actions of students and staff.

An educator[7] who "believed and had reasonable grounds for believing" that their copying constituted fair use cannot be sued for statutory damages.[8] Although it has not yet been tested by the courts, it is reasonable to conclude that reliance on the fair use guidelines will constitute reasonable belief and action by an educator. The Copyright Act specifically notes that instrumentalities of a state (such as a local board of education) cannot claim sovereign immunity for copyright infringement actions.[9]

In addition, educators should note that financial penalties can be attached for each infringement – in other words, each copy that is made. Thus, if 90 infringing copies were made for three classes, then a fine can be attached for each one.

The Internet & fair use guidelines

The Internet is both a boon and a bane from a copyright perspective. The advantage is that the Internet allows for easy, quick and inexpensive worldwide exposure for a creative work. The downside is that computer users can download and forward protected material at will – undetected – and there is little to stop individuals from electronically infringing on someone's copyright. For example, transferring a work from one computer to another is copying and potentially a copyright law violation.

Copyright and employment: Who is the owner?

In the employment context, if an employer has the right and ability to supervise the infringing action of an employee, and the employer has a direct financial interest in the exploitation of copyrighted materials, the employer may be held liable for the copyright infringement of its employees. This is true even where the employer lacks actual knowledge that the infringement is taking place.

7. The section includes the "employee or agent of a nonprofit educational institution, library or archives acting within the scope of his or her employment."

8. 17 U.S.C. 504

9. 17 U.S.C. 511

The standard that applies to students of colleges, universities and public schools has not been established. Students will often download Internet Web sites ("off-line browsing") and view the material at a later time. Another concern is when students download graphics, sound clips and text from other Web sites and "cut and paste" portions of a Web page into their own works. It could be argued that such use is a copyright infringement, and students should be discouraged from copying copyrighted materials and using the material in their schoolwork.

In some places, school districts are being challenged for copyright infringement in connection with mere everyday Internet use in classrooms and assembly spaces. Arguments are being made that *any* use of an Internet browser constitutes a reproduction of an original work, both in content and in presentation. This becomes even more ominous for school districts that broaden their information-gathering capabilities by deploying offline browsing, a technique that directs school district computers to connect to several designated Internet sites during off-peak times and download their contents onto the school district's internal network. Students retrieve the information and read it as if they were on the Internet, but the files actually are read from a local hard drive.

The advantages of offline browsing for school districts are two-fold. Speed is increased, since it is faster to read information from a local computer than live on the Internet. And, the practice gives school officials an extra degree of control, since students only have access to pre-screened Web sites, selected to be downloaded onto the school's computer system. Thus, the risk that students will inadvertently or intentionally access inappropriate material is reduced.

School districts faced with copyright challenges due to offline browsing can assert the fair use doctrine as a defense. The district might also consider an implied license defense, arguing that the copyright holder (*i.e.* the creator or author of the Web site) granted others an implied license to

Guidelines for off-air recordings of broadcast programming for educational purposes*

In March 1979, Congressman Robert Kastenmeier, chairman of the House Subcommittee on Courts, Civil Liberties, and Administration of Justice, appointed a Negotiating Committee consisting of representatives of education organizations, copyright proprietors and creative guilds and unions. The following guidelines reflect the Negotiating Committee's consensus as to the application of "fair use" to the recording, retention and use of television broadcast programs for educational purposes.

1. A broadcast program may be recorded off-air simultaneously with broadcast transmission (including simultaneous cable retransmission) and retained by a non-profit educational institution for a period not to exceed forty-five (45) consecutive calendar days after recording. When time expires, all off-air recordings must be erased or destroyed immediately.
2. Off-air recordings may be used once by teachers in the course of relevant teaching activities, and repeated once only when instructional reinforcement is necessary, in classrooms and similar places devoted to instruction within a single building, cluster or campus.
3. Off-air recordings may be made only at the request of teachers, and may not be regularly recorded in anticipation of requests. No broadcast program may be recorded off-air more than once at the request of the same teacher, regardless of the number of times the program may be broadcasted.
4. A limited number of copies may be reproduced from each off-air recording to meet the legitimate needs of teachers. Each such additional copy shall be subject to all provisions governing the original recording.

* House Report on Piracy and Counterfeiting, H.R. 495, 97th Cong. 1st Sess., at 8-9.

copy materials placed on the Internet, at least for their own personal use.[10] Note, however, if there is a statement on the site saying there is no implied license, then this argument might be ineffective.

Copyright on the Internet

The same prohibition on copying copyrighted materials applies to materials available over the Internet.

✘ The ease of copying materials from the Internet should not be used as an excuse for violating the copyright of others.

Exemptions under copyright law

Public education enjoys three important exemptions under the Copyright Act: face-to-face teaching; educational broadcasting; and non-profit performances. Unlike the fair use standards, the exemptions are relatively simple to understand without the benefit of guidelines.

FACE-TO-FACE TEACHING ACTIVITIES

Section 110 (1) of the Copyright Act excludes school performances from a copyright owner's control over the public performance or display of a work. An owner's copyright is not infringed when there is a:

> *Performance or display of a work by instructors or pupils in the course of face-to-face teaching activities of a non-profit educational institution, in a classroom or similar place devoted to instruction, unless in the case of a motion picture or other audiovisual work, the performance or the display of individual images, is given by means of a copy that was not lawfully made under this title, and that the person responsible for the performance knew or had reason to believe was not lawfully made.*[11]

Under this exemption, a teacher may read, perform or display a copyrighted work, as long as the conditions are met. First, the activity must take place "face-to-face." Although use of "devices for amplifying sound and for projecting visual images" is permitted, the instructor and pupils must be present in the same building or general area. According to Congress, this exemption is intended to exclude broadcasting or other transmissions from an outside location into classrooms.

Next, the lesson must be taught by "instructors." Congress included guest lecturers in this definition, but specifically excluded "performance by actors, singers or instrumentalists brought in from outside the school or to put on a program."[12]

Lastly, the instruction must occur in a "classroom or similar place devoted to instruction" for students. Therefore, "performances in an auditorium during a school assembly, graduation ceremony, class play or sporting event, where the audience is not confined to the members of a particular class, would fall outside the scope" of the exemption.[13]

10. See generally *McCoy v. Mitsubishi Cutlery, Inc.* 67 F.3d 917 (Fed. Cir. 1995)(manufacturer of patented knives under agreement with patentee had an implied license, and could resell knives under Texas law as a self-help remedy when the patentee refused to pay).

11. 17 U.S.C. 110(1)

12. H.Rep. No. 94-1476 (1976)

13. H.Rep. 94-1476, 94th Cong., 2d Sess., 85-86 (1976) Under certain conditions, however, the performance may be classified as a "non-profit performance" and be exempted under that provision.

INSTRUCTIONAL BROADCASTING

Section 110 of the Act also exempts certain instructional broadcasts from copyright infringement. Specifically, Section 110(2) states that "the performance of a nondramatic literary or musical work or display of a work by or in the course of a transmission"[14] is not an infringement of copyright.

Unlike the exemption for face-to-face teaching, the instructional broadcasting exemption limits the types of copyrighted works that can be used. "Nondramatic literary or musical works" would exclude an opera, musical comedy or motion picture. An owner's permission would be required in order to transmit these works.

Moreover, the performance or display must occur in a specific context. First, the statute states that it must be part of the "regular systematic instructional activities of a governmental body or a non-profit educational institution." Secondly, the performance must be "directly related and of material assistance to the teaching content of the transmission." Any such transmission must be "primarily" (rather than "solely") for reception in classrooms. Therefore, broadcasts which can be received by persons other than students are permissible. Lastly, the transmission must be received by officers or employees of a governmental body as part of their official duties or by persons who, because of "their special circumstances or disabilities," are unable to attend regular classrooms. For example, students who receive home and hospital instruction as well as employees who participate in staff development activities would fall into this category.

NON-PROFIT PERFORMANCES

The Act excludes non-profit performances from copyright control when: the work performed is a nondramatic literary or musical work; the work is not electronically transmitted to the public; and there is no payment of a fee for the performance to the performers or promoters. Last, the exclusion provides that no admission charge may be assessed, or that the proceeds collected must be used exclusively for educational, religious or charitable purposes and not for private financial gain.

Congress' purpose in limiting monetary gain was to "prevent free use of copyrighted material under the guise of charity where fees or percentages are paid." However, the legislative history specifically noted that school performances, where teachers were paid annual salaries, would not be considered "payment of a fee to performers." For example, a school band concert, where the band director receives a stipend for her work, would not be subject to copyright control as long as the other conditions of the section are met.

DURATION OF COPYRIGHT PROTECTION

Copyright protection, or an owner's exclusive control, is not perpetual. One of the law's goals is to

Example 3. How long does copyright last?

Harriet Jacobs is the faculty advisor for the drama productions for Harlem High. She wants to produce two plays: *Taming of the Shrew*, written by William Shakespeare in 1594, and *Raisin in the Sun*, written by Lorraine Hansberry in 1957.

Answer: Under the Act, Zora would not have to seek permission to produce Shakespeare's play. However, the Hansberry work is still protected by copyright. She would have to seek permission from Hansberry's heirs.[1]

1. Professor Laura Gassaway, University of North Carolina, has written a helpful table to determine whether a work has passed into the public domain. It is found at *http://www.unc.edu/~unclung/public-d.htm*.

14. "To transmit a performance or display is to communicate it by any device or process whereby images or sounds are received beyond the place from which they are sent." 17 U.S.C. 101.

promote the public good. In order to foster this goal, the private right possesses specific time limits. Without such limits, the owner's control might prevent any access by the public.

The Sonny Bono Copyright Term Extension Act, S. 505 P. L. 105-298 (signed into law on October 27, 1998) extends the term of copyright protection of work created on or after January 1, 1978. For individual authors, term of protection is life of the author plus 70 years. For corporate creators or for joint works of authorship, the term is 95 years after the date of first publication, or 120 years, which ever expires first. Once a work no longer receives copyright protection, it is considered to be part of the "public domain" and may be reproduced, copied or performed without seeking the author's permission.

The Copyright Term Extension Act includes an exception for libraries, archives and not-for-profit schools. These organizations may, during the last 20 years of a copyright term, "reproduce, perform, distribute, or display [a work] in facsimile or digital form" if for the purposes of preservation, scholarship or research. However, schools are restricted from taking these actions if the work is still subject to commercial exploitation, if a copy can be obtained at a reasonable price, or if the copyright owner has given notice that the work cannot be used.

Copyright Ownership

In most cases, the owner of a copyright is also the creator of a copyright. However, when a work is "prepared by an employee within the scope of his or her employment,"[15] the employer, rather than the creator, retains the exclusive rights of ownership. The work is considered a "work made for hire." In such cases, the owner of the copyright may be an individual or an entity, such as a local board of education. The United States Copyright Office has stated that works such as a newspaper article written by a staff journalist for publication, a software program created by a staff programmer for a computer corporation, or a musical arrangement for a music company produced by a salaried arranger on staff would be examples of works made for hire. In general, a court will examine: whether the employee's status is related to the nature of the work that has been created; whether the work performed by the employee is the employer's regular business; whether the employer withholds taxes for the employee; and whether the employer has control over the employee.[16] However, employment alone does not necessarily determine a work made for hire.[17]

SAMPLE POLICY STATEMENT

Ownership of products

Unless there is a specific agreement to the contrary, products created within the scope of employment relationship shall be the property of the Board of Education. Student work, unless created while the student is working for the school district, is the property of the individual student. Unless a student gives specific direction to the contrary, the school district may display notable student work created during the same school term or school year in non-electronic educational contexts (e.g., posting on a school bulletin board or at a school show). In the opinion of the Board of Education, such limited educational posting constitutes fair use.[1]

1. This point has never been litigated. It is an attempt to avoid asking for permission from students prior to displaying student work. Because it is unlikely that student work will have any economic impact, it is unlikely that limited posting for educational purposes will constitute infringement. However, you should discuss this issue fully with your school attorney.

15. 17 U.S.C. 101

16. *See generally Community for Creative Non-Violence v. Reid*, 490 U.S. 730 (1989), for a discussion of these factors.

17. *See Newark v. Beasley*, 883 F. Supp. 3 (D.NJ. 1995)(police officer who created an anti-violence curriculum as a result of his lectures on behalf of the police department owned the copyright in the curriculum).

Boards of Education, like other employers, have the option of granting copyrights to their employees, even when the works could be considered works made for hire. Any such option should be clearly noted in your school board's policy.

The issue of ownership of faculty-created works has never been litigated in the public school context. However, several items teachers create during the ordinary course of employment may or may not be considered works made for hire. For example,

> Suppose Zora decides to try to market the lesson plans that have brought her acclaim throughout the district. Would the Renaissance Board of Education be correct if it asserted that the plans are the property of the school board, not the individual employee?

Zora is clearly an employee of the school system who has created the lesson plans during the ordinary course of her employment. However, Zora could argue that the plans were created for her personal benefit – not to be used or endorsed by the entire school district. Unlike the computer programmer who was hired to write computer programs, or the newspaper reporter who was hired to write newspaper feature articles, Zora was *not* hired to write lesson plans, she was hired to teach. Yet, one could argue that a teacher cannot deliver an adequate lesson without developing a plan. In some jurisdictions, teachers are required to submit their lesson plans to the principal as part of their employment agreement and it is one of the criteria upon which a teacher is evaluated. Such an arrangement would strengthen the contention that the school district was the owner of the lesson plan.

The following example is illustrative:

> Suppose Zora's demonstration lesson is videotaped by the school district's administration. The school board decides to package the tape, together with curricular materials, to market to other school districts. The Board also plans to use the tape in teacher training sessions. It is likely that the school district, not Zora, would own the tape of the lesson.[18]

COPYRIGHT AND SCHOOL EMPLOYEES

Suppose Zora's cousin, Janie, is Web master for Harlem High School. The position, like those of coach and class advisor, carries a stipend negotiated through the district's collective bargaining agreement. Janie designs the school's award-winning Web page.

Who owns the copyright?

Answer: Because Janie has designed the Web page as a part of her employment, the school district owns the copyright in the Web page.

This is an issue your school board should discuss fully prior to adopting a policy on the ownership of copyrighted materials.

Some courts have carved out a "teacher exception" to the works for hire doctrine that "protects professors and like employees from having to assign the rights to their works to their universities."[19] This is primarily a higher education concept, however, and has not been applied in the elementary-secondary school context.

18. *Quintanilla v. Texas Television, Inc.*, 139 F.3d 494 (5th Cir. 1998)

19. Merges, et. al, "Intellectual Property in the New Technological Age, (1997), p. 398; *citing Hays v. Sony Corp. of America*, 847 F.2d 412, 416 (7th Cir. 1988); *Weinstein v. University of Illinois*, 811 F.2d 1091, 1093-94 (7th Cir. 1987); *but see University of Colorado Found. V. American Cyanamid*, 880 F. Supp. 1387 (D. Colo. 1995) (assuming academic article written by university professors was a work for hire).

STUDENT OWNERSHIP OF COPYRIGHT

A different set of rules applies to students. Even if a work is created within the classroom, the presumption is that the student holds the copyright and thus controls use of her or his creation. The Fort Smith Special School District in Arkansas found that out the hard way when it published – without permission – several writing projects by journalism students. In *Dodd v. Fort Smith Special Sch. Dis.*, 666 F.Supp 1278 (W.D. Ark. 1987), the Court ruled in favor of the teacher and her students and against the school district, which substantially copied from the manuscripts without giving credit. Although that case was not decided under the Copyright Act (since at that time registration was a requirement to initiate a copyright lawsuit), the same principles would likely apply today.

Copyright in the digital age

THE DIGITAL MILLENNIUM COPYRIGHT ACT OF 1998

On October 27, 1998, President Clinton signed into law the Digital Millennium Copyright Act of 1998 ("DMCA") (H.R. 2281, Public Law 105-304, 112 Stat. 2827). Although the Act attempts to make the law relevant to digital technology, the DMCA does not substantially alter the sections of the statute that apply to the education community. For example, fair use as it appears in Section 107 remains unchanged.[20]

The Act directs the Register of Copyrights, within six months of the signing of the Act, to recommend to Congress "how to promote distance learning through digital technologies." Additional legislation of interest to schools may result from the Register's recommendations.

Educational Fair Use Guidelines for Distance Learning

The distance learning guidelines apply to the performance of lawfully acquired copyrighted works not included under Section 110(2) of the Copyright Act (such as a dramatic work or an audiovisual work) as well as to uses not covered for works that are included in Section 110(2).

The covered uses are:

(1) live interactive distance learning classes (i.e., a teacher in a live class with all or some of the students at remote locations) and

(2) faculty instruction recorded without students present for later transmission. The guidelines apply to delivery via satellite, closed circuit television or a secure computer network. They do not permit circumventing anti-copying mechanisms embedded in copyrighted works.

Fair Use of Digital Technologies

While Congress has declined to determine specifically how fair use would apply to the digital age, the Conference on Fair Use (CONFU) began a study of the matter in 1994.[21] CONFU, composed of 93 organizations, compiled proposed guidelines for use of copyrighted materials in the non-profit education arena. But by its final meeting in 1997, some participating groups still were not convinced that the standing proposal was the best possible set of guidelines

20. Several education organizations, including NSBA, asked Congress for language that would specifically note that fair use applied to the digital media. Their attempts were unsuccessful.

21. The National Information Infrastructure Task Force, created by President Clinton and under the direction of the Department of Commerce, established the Working Group on Intellectual Property. It was this Working Group that convened the Conference on Fair Use to develop guidelines for the fair use of digital technology.

for education users. Thus, no one set of guidelines was endorsed by all of the groups in the conference. In general, users felt the guidelines were overly restrictive and copyright owners felt they gave away too much.

CONFU produced four sets of guidelines: *Fair Use Guidelines for Educational Multimedia*,[22] *Educational Fair Use Guidelines for Distance Learning*, *Statement on the Use of Copyrighted Computer Programs (Software) in Libraries* and *Guidelines for Digital Images*.[23] Although the Multimedia Guidelines have been opposed by many prominent education organizations,[24] no alternatives have been presented. Because of the lack of consensus, much of the terrain covered by CONFU remains a question mark for now. School districts that adopt CONFU guidelines should not hold the illusion that it provides a legal safe harbor. It does not, and a district might still find itself in a lawsuit challenging its electronic copying practices.

For more information on CONFU, consult the CONFU final report, *http://www.uspto.gov/web/offices/dcom/olia/confu/*. For helpful interpretation, see the University of Texas site, http://www.utsystem.edu/OGC/IntellectualProperty/confu.htm. Another good source for general information on copyright is the Copyright Management Center at Indiana University, http://www.iupui.edu/it/copyinfo/.

Stepping into the breach was the American Library Association, a non-profit education organization of 57,000 public, school, academic and specialized librarians, library educators, library trustees, and friends of libraries. The group agreed to assist in the development of "User Community Principles" and educator and librarian-generated "Best Practices" concerning fair use, distance learning and other activities supported by current copyright law. The statement, which included other principles, was endorsed by many education groups, including the National School Boards Association and the National Education Association.

SPECIFIC DIGITAL TECHNOLOGY: SOFTWARE

Software is protected by the Copyright Act as a "literary work." As such, an owner retains the right to control its copying[25] and distribution. Unlike a book or play, however, the fair use of software is almost impossible to quantify. That is, it is rare that only portions of a software program can be used. Therefore, software owners generally issue licenses to individuals. These licenses have specific conditions and usually limit the number of terminals or the site where the software may be used. Because software is protected by copyright law, your school district may be able to limit its liability by:

- Prohibiting staff and students from copying software licensed to the school system
- Prohibiting staff and students from loading personal software on equipment owned by the school district
- Requiring staff and students to adhere to the school district's software licenses

22. The Consortium of College and University Media Centers (CCUMC) presented the Multimedia Guidelines to CONFU, which in turn recommended their adoption.

23. It should be noted that while the multimedia guidelines were drafted with the participation of the National School Boards Association, NSBA specifically declined to endorse these guidelines.

24. In addition to NSBA, the American Association of School Administrators, American Association of State Colleges and Universities, American Council on Education, National Association of Elementary School Principals, National Association of Secondary School Principals and National Education Association have opposed the Multimedia Guidelines.

25. 17 U.S.C. 117 excludes from infringement the copying of computer programs for archival purposes as well as the copying that is necessary in order to adapt the program for specific uses or hardware.

DISTANCE LEARNING

In some cases, the CONFU distance learning guidelines do not apply to specific materials because no permission is required, either because the material to be performed or displayed is in the public domain, or because the instructor or the institution controls all relevant copyrights. In other cases, the guidelines do not apply because the copyrighted material is already subject to a specific agreement. For example, if the material was obtained pursuant to a license, the terms of the license apply. If the institution has received permission to use copyrighted material specifically for distance learning, the terms of that permission apply. Following are edited excerpts from CONFU's November 18, 1996 revised draft statement on:

Educational fair use guidelines for distance learning

Performance & Display of Audiovisual and Other Copyrighted Works

- *TRANSMISSION (DELIVERY):* Transmission must be over a secure system with technological limitations on access to the class or program such as a PIN number, password, smartcard or other means of identification of the eligible student. (Guideline 4.1)
- *RECEPTION:* Reception must be in a classroom or other similar place normally devoted to instruction or any other site where the reception can be controlled by the eligible institution. In all such locations, the institution must utilize technological means to prevent copying of the portion of the class session that contains performance of the copyrighted work. (Guideline 4.2)
- *ONE TIME USE:* Performance of an entire copyrighted work or a large portion thereof may be transmitted only once for a distance learning course. For subsequent performances, displays or access, permission must be obtained. (Guideline 5.1)

The school receiving the transmission may record or copy classes that include the performance of an entire copyrighted work, or a large portion thereof, and retain the recording or copy for up to 15 consecutive class days (i.e., days in which the institution is open for regular instruction) for viewing by students enrolled in the course. Access to the recording or copy for such viewing must be in a controlled environment such as a classroom, library or media center, and the institution must prevent copying by students of the portion of the class session that contains the performance of the copyrighted work. If the institution wants to retain the recording or copy of the transmission for a longer period of time, it must obtain permission from the rights holder or delete the portion which contains the performance of the copyrighted work. (Guideline 5.2.1)

Four examples of when permission is required:

1. Commercial uses: Any commercial use including the situation where a school is conducting courses for a for-profit corporation for a fee. (Guideline 7.1)
2. Dissemination of recorded courses: A school offering instruction via distance learning under these guidelines wants to further disseminate the recordings of the course or portions that contain performance of a copyrighted work. (Guideline 7.2)
3. Uncontrolled access to classes: A school wants to offer a course or program that contains the performance of copyrighted works to non-employees. (Guideline 7.3)
4. Use beyond the 15-day limitation: A school district wishes to retain the recorded or copied class session that contains the performance of a copyrighted work not covered in Section 110(2). (It also could delete the portion of the recorded class session that contains the performance). (Guideline 7.4)

The Digital Millennium Copyright Act enables software publishers, music and film studios and others to keep their non-printed, copyrighted materials from being distributed for free on the Internet, where markets could be undermined.

Although the Digital Millennium Copyright Act does not specifically make fair use applicable to works appearing in digital media, it makes no changes to the fair use doctrine or other privileges and rights already accorded users under current copyright law.

The law does, however, prohibit the "circumvention" of any effective "technological measure," such as a password or form of encryption, used by a copyright holder to restrict access to its materials. It also prohibits the manufacture of any device or offering of any service primarily designed to defeat an effective "technological protection measure." The first restriction becomes effective in October 2000 and the second in April 2000.

EDUCATOR FAIR USE OF COPYRIGHTED DIGITAL IMAGES
—USE BY EDUCATORS, SCHOLARS AND STUDENTS
Drafted by CONFU December 3, 1996

- An educator may display digital images for educational purposes, including face-to-face teaching of curriculum-based courses, and research and scholarly activities at a non-profit educational institution. (Guideline 3.1.1)

- An educator may compile digital images for display on the institution's secure electronic network to students enrolled in a course given by that educator for classroom use, after-class review, or directed study, during the semester or term in which the educator's related course is given. (Guideline 3.1.2)

- *Use of Images for Peer Conferences.* Educators and students may use or display digital images in connection with lectures or presentations in their fields, including uses at non-commercial professional development seminars, workshops, and conferences where educators meet to discuss issues relevant to their disciplines or present works they created for educational purposes in the course of research, study, or teaching. (Guideline 3.2)

- *Use of Images for Publications.* These guidelines do not cover reproducing and publishing images in publications, including scholarly publications in print or digital form, for which permission is generally required. (Guideline 3.3)

- Educators and students may digitize lawfully acquired images to support the permitted educational uses under these guidelines if the inspiration and decision to use the work and the moment of its use for maximum teaching effectiveness are so close in time that it would be unreasonable to expect a timely reply to a request for permission. (Guideline 4)

- Images digitized for spontaneous use do not automatically become part of the institution's image collection. Permission must be sought for any re-use of such digitized images or their addition to the institution's image collection. (Guideline 4)

Statement on use of copyrighted computer programs (software) in libraries

Drafted by CONFU on September 6, 1996

Seven possible scenarios involving schools & copyrighted software

1. A school library purchases a spread sheet program for managing accounts payable, and the Information Systems director adapts the program so it can be used on the library's computers. (Guideline Scenario 1a)

Acceptable: This use qualifies for the Section 117 exemption. The owner of a lawfully acquired copy of a computer program is permitted to make an adaptation of a computer program "as an essential step in the utilization of the computer program in conjunction with a machine and that it is used in no other manner." If the library licenses, rather than purchases, the program, then it should refer to the license agreement or contact the copyright owner before making an adaptation.

2. The head librarian of a school licenses a spread sheet program specifically for managing the library's accounts payable, but the school district business office uses a different program. The library administrator prepares monthly reports with its special program and sends them to the district's central office on diskette or via e-mail with a copy of the library's spreadsheet program so that the business office can download the reports. (Guideline Scenario 1b)

Unacceptable: No fair use defense or statutory exemption is available. Because the spreadsheet program copy sent to the district's central office was not lawfully made, this does not qualify for the non-profit library lending exemption, or the non-profit educational lending exemption permitting transfer of possession of computer programs to "faculty, staff, and students."

3. Assume the same facts as in (2) above, except that the library administrator does not send the monthly reports with a copy of the library's spreadsheet program, but rather reformats the monthly report into text for transmission to the district's central office. (Guideline Scenario 1c)

Acceptable: Fair use defense or statutory exemptions are not necessary. Because the library administrator has not made an unauthorized reproduction or distribution of the spreadsheet program, there is no copyright infringement.

continues on next page

4. A school library purchases a single-machine license for a spreadsheet program to be used in calculating employee payroll. A library employee opens the sealed envelope containing the CD-ROM or diskette and installs the computer program on a computer without reading the license agreement. Later, he makes a copy of the program and gives it to a colleague on the library staff, who loads it on her computer. (Guideline Scenario 1d)

Unacceptable: No fair use defense exists under Section 107. The library has infringed the copyright by making an unauthorized reproduction of the computer program, and there are no other statutory exemptions available.

5. A librarian busy cataloging and archiving important materials decides to work at home. To keep track of her hours, she makes a copy of the spreadsheet program installed on her office computer and takes it home to install on her home computer. (Guideline Scenario 1e)

Unacceptable: No fair use defense or statutory exemption is available. Because many end-users now want to work at home as well as the office, many business application publishers now offer "single user licenses," which permit the licensee to install and use the computer program on both an office and a home computer provided the two copies are not in use simultaneously.

6. A librarian licenses and installs a spreadsheet program to manage her budget. Two years later, the librarian licenses a functional upgrade for the program, installs it on her office computer, and installs the older version alone on her home computer. (Guideline Scenario 1f)

Unacceptable: No statutory exemption or fair use defense exists if a valid license for the functional upgrade prohibits transfer of the older version to another machine or another user. Software license agreements distinguish between functional upgrades of licensed software and the current version licensed by new customers. Because functional upgrades are licensed on the assumption the customer has already licensed a previous version of the software, their prices are usually about two-thirds lower than the price of the current title for new customers. Therefore, most functional upgrade licenses restrict or prohibit the transfer of the previous version to another user or machine.

7. Assume the same facts as in (6), except the librarian obtains a full-price license to the new version of the program, rather than the less expensive functional upgrade, for her office computer, and installs the older version alone on her home computer. (Guideline Scenario 1g)

Acceptable: It is unnecessary to consider fair use or statutory exemptions. Because the librarian has licensed two complete and independent programs, the copyright in the programs has not been infringed.

Policy considerations for your school board

School districts can avoid litigation by requesting permission for use of copyrighted materials.[26] However, this method is costly, time consuming and inefficient. Publishers generally respond within four to six weeks, and few instructors have the luxury of such an extended period of time.

In discussing the adoption of the fair use guidelines and ways to avoid exposure to copyright infringement, your school board should:

- Carefully review the current use of copyrighted materials in the classroom. Does your school board have a policy on the use of copyrighted materials? Are staff members aware of their liability? Have you adopted any of the CONFU guidelines?
- Make certain the school's Acceptable Use Policies for student and employee use of technology include copyright compliance as a condition of access to technology.
- Consider designating an individual to coordinate copyright requests for the school district.
- Train staff on the basic requirements of intellectual property law.
- Explain the consequences of copyright infringement to both students and staff members.
- Consult with your school board counsel on the adoption of the CONFU guidelines.
- Establish clear standards for the use of copyrighted materials on the World Wide Web.
- Disseminate widely any copyright policy[27] or procedure you adopt.

Conclusion

The sudden, widespread use of technology offers one of the most exciting – and daunting – challenges to public education since the advent of the Industrial Age. Public school policy makers have the opportunity to shape the minds of the generation that will propel society forcefully into the next millennium. While the legal issues accompanying these new technologies are, in many cases, undecided, this should not prevent the careful board of education from meeting the challenges that lie ahead.

Margaret-Ann F. Howie is legal counsel to the superintendent of the Baltimore County, Maryland Public Schools. She advises the superintendent and senior staff on issues ranging from students' rights and personnel to open meetings and intellectual property. She is recognized for her expertise in the areas of student discipline and school violence.

26. A sample permission letter is included at the end of this chapter.

27. NSBA maintains a policy network, with sample policies from various school districts. Many state school boards associations and state departments of education offer a similar service.

Resources & Sample Copyright Permission Request

Print

- *Nimmer On Copyright*. The most comprehensive treatise available (ten volumes). This is a good library resource for your school district's legal counsel.

- Robert Gorman and Jane Ginsburg, *Copyright for the Nineties*. A more compact casebook on copyright law. (One volume)

- Margaret-Ann F. Howie. *Copyright Issues in Schools* (LRP, 1997)

Internet

United States Copyright Office, Library of Congress.
http://www.loc.gov/copyright
Copyright Office Circular 21, which contains the Guidelines for Classroom Copying, Music and Off-Air Broadcasting, can be found at:
gopher://marvel.loc.gov:70/00/ftppub/copyright/circs/circ21

Conference on Fair Use report. (Includes text of the new fair use guidelines as well as the nonlegislative report)
www.uspto.gov/web/offices/dcom/olia/confu/conclutoc/html

Copyright Management Center, University of Texas System,
Office of the General Counsel.
This Web site explains fair use and the education exemptions in a clear and easy to understand way. Users should remember, however, that much of what is done on the higher education level is not applicable to public education.
http://www.utsystem.edu/OGC/IntellectualProperty/cprindex.htm

Music Library Association.
Contains a good summary of fair use and some useful FAQs.
http://www.musiclibraryassoc.org/Copyright/guidemla.htm

Stanford University Libraries.
Contains good information and links on the issue of fair use.
http://fairuse.stanford.edu

United States House of Representatives Internet Law Library.
http://www.pls.com:8001/his/95.htm

University of North Carolina.
Professor Laura Gasaway's chart is a good resource for determining when works pass into the public domain.
http://www.unc.edu/unclng/public-d.htm

Cornell University Legal Information Institute
Full text of the Copyright Act
http://www.law.cornell.edu/usc/17/

David E. Sorkin, Professor, The John Marshall Law School
Schools, the Internet, and the Law: Legal and Policy Concerns for Schools Using the Internet
http://www.mcs.net/~sorkin/internet/

Janis H. Bruwelheide, Professor, Montana State University-Bozeman
The Copyright Primer for Librarians and Educators, 2d Edition
http://www.homepage.montana.edu/~iedjb/index.htm

Columbia University
http://www.ilt.columbia.edu/projects/copyright/index.html

Groton Connecticut Public Schools
Includes links to Acceptable Use Policies
http://www.groton.k12.ct.us/www/pol/cpright.htm

U.S. Government Legislative Information on the Internet
Database of law and other legislative information
http://thomas.loc.gov

SAMPLE LETTER

[To appear on school or school district letterhead stationery and to include sender's appropriate fax number and other contact information]

REQUEST FOR COPYRIGHT PERMISSION

Permissions Department
Publisher

Re: Permission to Use Copyrighted Materials

Dear Sir/Madam:

Kindly consider this letter as a request to use the following copyrighted materials:

[DESCRIBE HERE, INCLUDING TITLE, PAGE NUMBERS AND DATE OF PUBLICATION. IF POSSIBLE, INCLUDE A COPY.]

These materials will be used for

[DESCRIBE CLASS OR PUBLICATION IN WHICH THE MATERIAL WILL BE USED, INCLUDING NUMBER OF STUDENTS, DURATION, ETC.]

Should you have a specific copyright notice, please specify it here:

_____

_____

_____

A duplicate copy of this letter has been enclosed for your convenience. Kindly return a signed copy to my attention.

If you are not the copyright holder, kindly inform me to whom I must address my request.

Sincerely,

School Administrator or
Classroom Teacher

Permission Granted:

_____
Name (please print)

_____
Signed

_____
Title, Date

Appendix

PORNOGRAPHY, THE COMMUNICATIONS DECENCY ACT AND THE *RENO* DECISION

Sexually explicit material on the Internet ranges from modest to hard core. These files are created, named and posted in the same manner as material that is not sexually explicit, and may be accessed either deliberately or unintentionally during the course of an imprecise search. Once a provider posts its content on the Internet, it cannot prevent that content from entering a community.[1]

Software has been developed to help control the material that may be available on a computer with Internet access. This system may limit a computer's access to an approved list of sources that have been identified as containing no adult material; block designated inappropriate sites; or it may attempt to block messages containing identifiable, objectionable features. Currently available software has been developed that can screen for certain suggestive words or for known sexually explicit sites, but cannot screen for sexually explicit images. However, the Court found in *Reno* that there was evidence to indicate that a reasonably effective method was available for parents to prevent their children from accessing sexually explicit material and other material they believe is inappropriate for their children.[2]

The Court also noted that commercial pornographic sites charge their users for access and assign them passwords as a method of age verification, but that system was unreliable and would be burdensome for noncommercial sites.

The Communications Decency Act, 47 U.S.C. Section 223(a)(l)(B)(ii), imposed criminal penalties for the knowing transmission of obscene or indecent messages to any recipient under 18 years of age, and Section 223(d), which prohibits knowingly sending or displaying any message that, in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs.

The Court in *Reno v. American Civil Liberties Union* in 1997 held that the Communications Decency Act was overbroad and in violation of the First Amendment and distinguished its prior decisions in *Ginsberg v. New York* [3] and *F.C.C. v. Pacifica Foundation*.[4]

In *Ginsberg*, the United States Supreme Court upheld the constitutionality of a New York statute that prohibited selling to minors under 17 years of age material that was considered obscene to minors, even if it was not obscene as to adults. The Court noted that the rights of minors was not coextensive with that of adults, and held that the state had an independent interest in the well being of its youth and the authority of parents to rear their children. The Court noted that the statute upheld in *Ginsberg* was much more narrowly drawn than the Communications Decency Act (CDA). The Court noted that in *Ginsberg*, the New York statute did not prohibit parents from purchasing the material for their children.

Under the CDA, by contrast, neither the parents' consent nor even their participation in the communication would avoid the application of the CDA. Second, the New York statute applied only to commercial transactions, whereas the CDA contains no such limitation. Third, the New York statute narrowly defined material that was harmful to minors with the requirement that it be utterly without redeeming social importance for minors. The CDA fails to provide any definition of the term "indecent" as used in Section 223(a)(1) and omits any requirement that the patently offensive material covered in Section 223(d) lacks serious literary, artistic, political or scientific value. Fourth, the New York statute defined a minor as a person under the age of 17, whereas the CDA, applied to all those

1. *Reno v. ACLU*, 47 S.Ct. 2329, 2336 (1997).
2. Id.
3. 88 S.Ct. 1274 (1968)
4. 98 S.Ct. 3026 (1978)

under 18 years, including an additional year of those nearest majority.[5]

The court in *Reno* distinguished its decision in *Pacifica*, which upheld an order of the Federal Communications Commission prohibiting the broadcast recording of a 12-minute monologue entitled "Filthy Words." The Court noted there were significant differences between the order upheld in *Pacifica* and the CDA. First, the order in *Pacifica* was issued by the FCC, which regulates radio stations and their program content. Second, the CDA's broad categorical prohibitions are not limited to particular times and are not dependent on evaluation by an agency like the FCC familiar with the unique characteristics of the Internet. Also, unlike the CDA, the FCC's declaratory order was not punitive and contained no criminal penalties. Most significantly, the court held that the FCC's order applied to a medium (i.e., radio), which, as a matter of history, had received the most limited First Amendment protection in large part because warnings could not adequately protect the listener from unexpected program content. The Court noted that the Internet, however, had no comparable history, and the risk of encountering indecent material by accident was remote because of a series of affirmative steps required to access specific material.[6]

The Court concluded that while several prior cases have recognized special justifications for the regulation of the broadcast media, in part due to the scarcity of available frequencies and to radio's invasive nature, these factors are not present with respect to the Internet. The court noted that the Internet is not as invasive as radio or television. The Court noted that users seldom encounter content by accident and that sexually explicit images are preceded by warnings as to the content.[7]

The Court also noted that the Internet cannot be considered a scarce expressive commodity as television and radio are because it has relatively unlimited low cost capacity for communication of all kinds. The Court concluded, "... our cases provide no basis for qualifying the level of First Amendment scrutiny that should be applied to this medium."[8]

The Court noted that the CDA failed to utilize the test established by the United States Supreme Court in *Miller v. California*.[9] As a result, the Court noted that the CDA lacks the precision that the First Amendment requires when a statute regulates the content of speech. The CDA, the Court noted, effectively suppresses a large amount of speech that adults have a constitutional right to receive and to address to one another. That burden on adult speech is unacceptable if less restrictive alternatives would be at least as effective in achieving the legitimate purpose that the statute was enacted to serve. The Court stated:

> "It is true that we have repeatedly recognized the governmental interest in protecting children from harmful materials.... But that interest does not justify an unnecessarily broad suppression of speech addressed to adults."[10]

The Court noted that there was currently available user-based software that provide a reasonably effective method by which parents can prevent their children from accessing sexually explicit and other material which parents may believe is inappropriate for their children. The Court noted that this software would soon be widely available.[11]

The court observed that the CDA might put a parent who sent his 17-year-old college freshman information on birth control via e-mail in jeopardy if the child's college town — but not the child nor anyone in their home community — found the material indecent or patently offensive.

For these reasons, the United States Supreme Court held these provisions to be unconstitutional as to the terms "indecency" and "patently offensive." The court noted that there was no challenge to the application of the statute to obscene speech under the *Miller* definition. Therefore, the United States Supreme Court severed the term "or indecent" from the statute.[12]

5. *Reno* at 2341
6. Id. at 2341-42
7. Id. at 2342
8. Id. at 2344
9. 93 S.Ct. 2607 (1973)
10. *Reno* at 2346
11. Id. at 2347
12. Id. at 2348-2351

DEVELOPMENTS AFTER RENO

There has been a variety of proposed legislation in Congress aimed at putting the brakes on what many representatives and senators see as runaway access to unpalatable material. One rendition in Congress in 1999 would require all schools receiving federally subsidized Internet hookups to select and install computer software to block inappropriate materials.

In *American Library Association v. Pataki*,[13] the federal district court held that a New York statute prohibiting the transmission of material harmful to minors over the Internet was unconstitutional and that it unduly burdened interstate commerce in violation of the commerce clause of the United States Constitution. The court held that the New York statute improperly regulated conduct outside New York's borders and could subject Internet users to its standards of regulations. The court stated:

> "...an Internet user cannot foreclose access to her work from certain states or send differing versions of her communication to different jurisdictions...The Internet user has no ability to bypass any particular state. The user must thus comply with the regulation imposed by the state with the most stringent standard or forego Internet communication of the message that might or might not subject her to prosecution. For example, a teacher might invite discussion of 'Angels In America' from a newsgroup dedicated to the literary interest of high school students. Quotations from the play might not subject her to prosecution in New York, but could qualify as 'harmful to minors' according the community standards prevailing in Oklahoma. The teacher cannot tailor her message on a community-specific basis and thus must take her chances or avoid the discussion altogether."[14]

The court went on to state that haphazard and uncoordinated state regulation of the Internet would frustrate its growth and that, "The need for uniformity in this unique sphere of commerce requires that New York's law be stricken as a violation of the commerce clause." Id. at 183.

In *ACLU v. Miller*,[15] the federal district court issued a preliminary injunction barring the enforcement of a Georgia statute that made it a criminal offense to use a false name or a name other than your own on the Internet or to create unauthorized links to web sites with trade names or logos. The federal district courtheld that the statute violated the First Amendment rights of Internet users, and that it was overbroad, vague and not narrowly tailored to promote a compelling state interest. Id. at 1233.

Sexually explicit materials were broadly defined in a manner broader than the U.S. Supreme Court's decision in *Miller v. California*.[16] The court also criticized the provisions of the act, which required employees to obtain permission from the state agency since the statute did not allow for appeals and required the granting of such requests to be made public records.

The courts have upheld provisions in federal law, such as the Child Pornography Prevention Act of 1996, 18 U.S.C. Section 2256, which prohibits the transmission of child pornography over the Internet. In *Free Speech Coalition v. Reno*, the federal district court held that provisions of the federal statute were constitutional. The court held that the federal statute was not unconstitutionally vague and gave sufficient guidance to a person of reasonable intelligence as to what it prohibits.

13. 969 F.Supp. 160 (S.D.N.Y. 1997)

14. Id. at 183.

15. 977 F. Supp. 1228 (N.D.Ga. 1997)

16. 413 U.S. 15, 24 93 S.Ct. 2607 (1973)

Glossary of Technology Terms

ASCII – American Standard Code for Information Interchange. A set of alphanumeric and special control characters. ASCII files are also known as plain text files.

BPS – Bits per second. A measurement of the volume of data that a modem is capable of transmitting. Currently, a typical modem speed is 56Kbps (56,000 bits per second).

Bookmark – A pointer to a particular Web site. Within browsers, a user can bookmark interesting pages and then return to them easily.

Browser, browsing – A program run on a computer that allows one to view World Wide Web pages. Examples include Netscape, Microsoft's Internet Explorer and Mosaic.

Chat room – An online location where participants can exchange notes, converse and share data live as they type messages to one another.

Downloading – The electronic transfer of information from one computer to another, generally from a larger computer to a smaller one, such as from a server to a personal computer.

Electronic bulletin board – A shared file where users can enter information for other users to read or download. Many bulletin boards are set up according to general topics and are accessible throughout a network.

E-mail – Electronic mail is comprised of messages delivered via computer networks to individuals' online "mailboxes." One can send not only messages, but also files, artwork, sound and video. E-mail is used both as a noun and as a verb (i.e., I received her e-mail two days after I e-mailed her.)

E-mail group – An electronic mailing list used to share information about a topic of common interest. When a person subscribes to an e-mail group, he or she receives – and in many cases can send – e-mail messages for all participants to read. Participants usually subscribe via a central service, and lists often have a moderator who manages the information flow and content. Listserv®, a commercial product marketed by L-Soft International Inc., and Majordomo, which is *freeware*, are popular mailing list servers. The term "listserv" often is used incorrectly to refer to any mailing list server.

E-zines – Electronic magazines distributed over the Internet — sometimes called zines (pronouced "zeens").

FAQ – Frequently asked questions. A collection of common questions and answers on a particular subject.

Flame – An insulting message, perhaps even malicious, exchanged via e-mail or within *newsgroups*. A series of flames are known as *flame wars*. Sometimes a flaming missive is intentionally sent in such huge quantities that it becomes a burden to the recipient.

FreeWare – Software that is copyrighted but freely available for downloading and use. Compare with *shareware*.

GIF – Graphics interchange format. A common image format. Most images seen on Web pages are GIF files.

Home page – The main page of a Web site, usually where the site's items are listed for easy access. Also, the Web site that automatically loads each time the user launches a *browser*.

HTML – HyperText Markup Language. Used to author documents on the Web.

HTTP – HyperText Transfer Protocol. The Web's protocol that defines formatting and transmission of messages and how browsers and Web servers respond to commands.

Hyperlink – A connection between pieces of information within one document or two separate documents, possibly at different Web sites. Clicking with a mouse on one will take the user to the linked location.

Hypertext – A database system that allows text, graphics, sounds and other "objects" to be linked to each other – such as at a Web site or in a CD-ROM program.

Intellectual Property – A general reference to the legal rights granted to authors, artists, inventors and other creators to control the use and dissemination of their original ideas or unique way of expressing those ideas. Applies with equal force to the Internet and other technologies.

Internet – The Internet is a global network of millions of computers that provides access to a wide range of information housed on different Web sites and enables fast, inexpensive communication among people.

Intranet vs. Internet– Internet documents and information are available to anyone in the world, except for items protected by security systems. Intranet documents and information are available only to computers within a specific network. Intranets are closed and secure; the Internet is open. Both intranets and Internet are based on *TCP/IP* protocols.

ISDN – Integrated services digital network. An international communications standard for high-speed transmission of voice, video and data over digital telephone lines.

ISP – Internet service provider. A company that provides a connection to the Internet via either a *dial-up connection* or a *direct connection*.

IP address – Internet protocol address. Every computer on the Internet has a unique identifying number, such as 111.0.11.0. IP addresses are assigned by the Inter NIC Registration Service (*http://www.internic.net*).

JPEG – Joint Photographic Experts Group, a common image format. Most of the images embedded into Web pages are *GIFs*, but sometimes, especially in art or photographic Web sites, one can click on the image to bring up a higher resolution JPEG version of the same image.

Link – Another name for a *hyperlink*. It is the place in a Web document where the viewer can click to travel or link to a different Web location. Links collectively make a web of information.

Listserv® – See *e-mail group* above.

MIDI – Musical instrument digital interface, a standard the music industry has adopted for controlling electronic musical devices, such as synthesizers.

Modem – A device for transmitting electronic signals between computers (which store information digitally) and analog telephone lines. The term is derived from "modulator-demodulator," describing what a modem does to signals. A cable modem operates over cable television lines.

MPEG – Motion Picture Experts Group. An industry group and the video compression standards and file formats they develop to produce excellent quality in relatively small files. Video files found on the Internet are commonly stored in the MPEG format. Also, full-length movies housed on CD are usually stored in the MPEG format.

Multimedia – A combination of media types such as graphics, animation, audio and/or video in a single document.

Newsgroup – An online discussion group covering a shared interest of participants. A "newsreader" program, such as those available at some Web browser sites, is required to view and post messages to the group. Unlike with an *e-mail group*, access is not limited to a list of individuals.

Search Engines – Search engines enable computer users to research a topic, in an organized and methodical way, on the Internet. Examples of common search engines are AltaVista (*http://www.altavista.com*) and Lycos (*http://www.lycos.com*).

Server – A computer or other device that manages a network's resources. See *Web server*.

Shareware – Microcomputer software, distributed through public domain channels, for which the author requests compensation from those who use it.

Spam – A slang term for e-mail that is the electronic equivalent of junk mail. Usually advertisements, jokes, or notices of no real value to the recipient.

T-1 LINE – A high speed, high-bandwidth telephone connection. It carries 1.544 megabits per second of data and is capable of handling tens of thousands of requests for information daily. Businesses often connect to the Internet using T-1 lines.

TCP/IP – Transmission Control Protocol/Internet Protocol is a combined set of protocols that perform the transfer of data between two computers. TCP monitors and ensures correct transfer of data. IP receives the data from TCP, breaks it up into "packets," and ships it off to a network within the Internet. TCP/IP is also used as a name for a protocol that incorporates these functions and others.

URL – Uniform Resource Locator. A standardized resource address system used on the Web. The URL describes everything that is necessary for a Web browser to locate a resource. It defines the name of the computer, the site it is housed on, the path, and the file name.

Webmaster – An individual who manages a Web site, possibly charged with site design and maintenance, response to queries and monitoring use.

Web server – The host computer that houses a home page and Web site. It allows full time access to the site.

Web site – The combination of a home page and any additional Web pages that represent a school district, individual, organization or business in the Internet community. It can offer text documents, graphics, video, audio and interactive forms.

World Wide Web – The Web, a system of Internet servers supporting documents formatted in *HTML* so that elements – such as text, graphics, audio and video items – can be linked when users click a mouse on designated spots at Web sites. Web *browsers* are used to access the World Wide Web.

NSBA Council of School Attorneys
Publications List

April 1999

School Law in Review 1999 This digest of papers presented at the 1999 Annual School Law Seminar includes the following topics: preventing threats of violence in schools from turning into a tragedy; the attorney's role in responding to violence: a case study of Jonesboro, AR; preparing to handle the news media during a crisis; legal implications of high stakes testing; what to ask – legal and policy issues in conducting effective background investigations; what to tell – legal and policy problems with references about former employees; the attorney-client privilege: challenges to a traditional value; bargaining and labor relations issues of school reform; collective bargaining and school reform; public relations aspects of managing a strike; IEP development and placement; practical suggestions to educators: avoiding procedural violations of the IDEA; and disciplining the disabled: an analysis of the law and court and hearing officer interpretations under the reauthorized IDEA. 154 pages. ISBN 0-88364-223-9 (List $35, Council members - first copy free. National Affiliates and additional Council copies $28).

A School Law Retreat Notebook (October 1998) This loose-leaf trial notebook is a compilation of the presentations given at the Council's October 1998 advocacy seminar in San Antonio, Texas. Topics include drug testing of school district employees, Religious Freedom and Equal Access Act, as well as the future of affirmative action, legal issues in employment, and the Fair Labor Standards Act. It also includes new developments in special education, ethics for the school attorney, new developments in sexual harassment, school district policies on student use of the internet, and providing educational services to students in non-traditional settings. ISBN 0-88634-218-2 (List $200, National Affiliates and Council members $160).

Student-to-Student Sexual Harassment: A Legal Guide for Schools (April 1998) Addressing a complex legal and social issue, this monograph provides the school law practitioner and school leaders with information on how to prevent, respond to, analyze and defend student to student harassment claims. In addition to discusssing federal case law, it includes a section on policy development, advice on conducting investigation; tips for training, and analysis of the Office of Civil Rights Guidelines and appendices containing OCR documents, sample policies and forms and helpful check lists. 186 pages. ISBN 0-88364-216-6 (List $35, National Affiliates and Council Members $28).

Legal Handbook on School Athletics (March 1997) This monograph provides school attorneys, board members, administrators and athletic directors with an understanding of the various legal issues that affect school athletic programs. Discussion of the law is supplemented with practical advice. Topics include: discipline of athletes: due process considerations, eligibility rules protecting high school athletes, participation of private school and disabled students, drug testing, Title IX, public school sports and religion, injuries during physical education classes and extra-curricular activities, spectator issues, student athletics and insurance issues, athletic personnel and volunteer issues. 120 pages. ISBN 0-88364-206-9 (List $35, National Affiliates and Council Members $28).

Selecting and Working With a School Attorney: A Guide for School Boards (April 1997) In today's world, getting good legal advice when problems arise and on how to avoid problems in the first place is a must for school boards. This book shows school board members how to select and to work effectively with a school attorney. Topics include: historical development of the role of the school attorney, hiring in-house counsel v. an outside attorney, selection, recruitment and retention of legal counsel, ethical issues in school board representation, evaluation and termination of school district counsel, the school attorney as a preventive law practitioner, how to work effectively with the school attorney. Also included in the appendices are sample policies, forms, agreements and checklists. 142 pages. ISBN 0-88364-209-3 (List $35, National Affiliates and Council Members $28).

Termination of School Employees: Legal Issues and Techniques (April 1997) Disputes over employee termination are the most common legal problem faced by schools. In order to assist school attorneys and officials in handling these disputes, this monograph addresses the legal issues and suggests effective techniques associated with proper termination of school employees. Topics include: employee performance documentation, evaluation, remediation, settlement agreements, public employee speech and off duty conduct, termination of drug/alcohol abusers, legal issues in trying a misconduct case, due process, and employment at will. 316 pages. ISBN 0-88364-210-7 (List $35, National Affiliates and Council Members $28).

Additional Council Publications
(See order form for more titles)

School Reform: The Legal Challenges of Change (April 1996) This monograph is intended to assist school attorneys in their efforts to advise school boards on the legal issues that accompany various reform measures. Covering such topics as school finance, choice, site-based management, privatization, alternative schools, charter schools and tenure reform, the discussion ranges from constitutional dilemmas to statutory issues to labor relations implications. Review of the law is supplemented with practical advice. 150 pages. ISBN 0-88364-202-6 (List $30, National Affiliates and Council Members $25).

Reasonable Accommodation of Disabled Employees: A Comprehensive Case Law Reference (February 1996) written by Brian Shaw. This reference book provides brief summaries of over 200 cases deciding reasonable accommodation issues under the Americans with Disabilities Act and Section 504 of the Rehabilitation Act of 1973. The summaries are arranged topically addressing: 1) general issues such as standards, knowledge of disability, suggesting an accommodation, burden of proof, and good faith defense; 2) over 20 different types of accommodations; and 3) undue hardship issues. A detailed table of contents and table of cases provide easy access to school attorneys looking for case law to help answer their clients' accommodation questions. 95 pages. ISBN 0-88364-200-X (List $15, National Affiliates/ Council of School Attorneys price $12).

Desk Reference on Significant U.S. Supreme Court Decisions Affecting Public Schools (Revised Edition 1996) by Gwendolyn H. Gregory, NSBA Deputy General Counsel. This desk reference is designed to serve as a "memory prompt" for attorneys and laymen alike on the name, citation and/or rule of law of a particular U.S. Supreme Court case. It contains virtually all cases in which a public school district was a party and a substantive decision was rendered, however it does not analyze the decision. It includes an extensive descriptive word index, table of cases with full parallel citations and table of constitutional and statutory provisions. 106 pages. ISBN 0-88364-135-6 (List $25, National Affiliates and Council members $20).

A School Law Retreat (October 1997) This looseleaf trial notebook is a compilation of the presentations given at the Council's October 1997 advocacy seminar in Phoenix, Arizona. Topics include: legal issues in employment, home schools and charter schools, discrimination against students: Title VI, IX and Section 504, ethics for school attorneys, school district records and management, new developments in special education, constitutional rights of students, and The Americans with Disabilities Education Act. 610 pages. ISBN 0-88364-213-1 (List $200, National Affiliates and Council Members $160).

Legal Guidelines for Curbing School Violence (March 1995). Addressing one of the most urgent problems in schools today, this publication covers such issues as search and seizure, metal detectors, students' due process rights, discipline of students with disabilities, tort and constitutional liability, hate speech, dress codes and gangs, keeping weapons out of schools and working with the criminal justice system. This comprehensive legal guide includes numerous sample policies. 162 pages. ISBN 0-88364-195-X (List $30, National Affiliates and Council Members $25).

Religion, Education and the U.S. Constitution (Revised edition March 1994) edited by Naomi Gittins. This edition includes the latest developments in the law, including the Supreme Court's decisions in *Zobrest*, *Lamb's Chapel* and *Lukumi*. This monograph is a compilation of articles written by Council members and focuses on the effect of the establishment and free exercise clauses of the first amendment and the constitutional issues surrounding accommodating employee religious beliefs, wearing of religious garb, curriculum content, school prayer/moment of silence, holiday observances, equal access, home school and much more. 198 pages. ISBN 0–88364–183–6 (List $25, National Affiliates and Council members $20).

School Board Member Liability Under Section 1983 (April 1992) by David B. Rubin, Piscataway, NJ (editor, Naomi E. Gittins, NSBA staff attorney). Like earlier editions published in 1981 and 1985, this monograph serves as a primer for both school board members and school attorneys on board member liability issues. The current version seeks to explain clearly and accurately in layman's terms the basics of civil rights law under Section 1983. It focuses on the types of claims most commonly brought under Section 1983 against school boards and presents factual circumstances and how the courts have applied the law in immunity defenses. 44 pages. ISBN 0-88364-134-8 (List $15, National Affiliates and Council members $12).

NSBA COUNCIL OF SCHOOL ATTORNEYS
PUBLICATIONS ORDER FORM
April 1999

·NSBA·

SHIP TO: (Please provide street address, not P.O. Box)

Name _____

Title _____

Organization _____

Street Address _____

City _____ State _____ Zip _____

Phone (_____) _____

BILL TO: (if other than ship to)

Name _____

Title _____

Organization _____

Street Address _____

City _____ State _____ Zip _____

Phone (_____) _____

❒ My check made payable to NSBA in the amount of $_____ is enclosed.

❒ Bill me using P.O. Number _____
PLEASE NOTE: Orders less than $30 must be paid in advance by check or credit card.

❒ My district is an NSBA National Affiliate, NA# _____

Please charge my: ❒ VISA ❒ MasterCard ❒ Amex

Card Number

_____
Authorized Signature Exp. Date

☐ **Check here to automatically receive new Council publications through the standing Order System. I understand I have 30 days to preview these publications and may return them at no risk or I may keep them and submit payment.**

Signature _____ Date _____

Order #	Title	Quantity	Member Price	Nonmember Price	Total
New 06-168-1	**School Law in Review 1999** (back issues available)		$28.00	$35.00	
New 06-166-1	**Student-to-Student Sexual Harassment: A Legal Guide for Schools**		$28.00	$35.00	
06-163-1	Termination of School Employees: Legal Issues and Techniques		$28.00	$35.00	
06-162-1	Selecting and Working With a School Attorney: A Guide for School Boards		$28.00	$35.00	
06-160-1	Legal Handbook on School Athletics		$28.00	$35.00	
06-158-1	School Reform: The Legal Challenges of Change		$25.00	$30.00	
06-156-1	Reasonable Accommodation of Disabled Employees: A Comprehensive Case Law Reference		$12.00	$15.00	
06-155-1	Desk Reference on Significant Supreme Court Decisions Affecting Public Schools (*Revised Edition*)		$20.00	$25.00	
06-152-1	Legal Guidelines for Curbing School Violence		$25.00	$30.00	
06-151-1	Environmental Law: Fundamentals for Schools		$12.00	$15.00	

BEST COPY AVAILABLE

Order #	Title	Quantity	Member * Price	Nonmember Price	Total
06-148-1	Child Abuse: Legal Issues for Schools		$20.00	$25.00	
06-147-1	Religion, Education, and the U.S. Constitution (*Revised Edition* - March 1994)		$20.00	$25.00	
06-143-1	Sexual Harassment in the Schools: Preventing and Defending Against Claims (*Revised Edition* - March 1993)		$20.00	$25.00	
06-142-1	Americans with Disabilities Act: Its Impact on Public Schools (March 1993)		$20.00	$25.00	
06-136-1	School Board Member Liability Under Section 1983		$12.00	$15.00	
06-122-1	School Discipline Policies & Procedures: A Practical Guide (*Revised Edition* – April 1990)		$20.00	$25.00	
06-121-1	Investigating Alleged Wrongdoing by Employees in the School Setting		$20.00	$25.00	
Trial Notebooks —					
06-167-1	**A School Law Retreat (October 1998) San Antonio, Texas**		$160.00	$200.00	
06-164-1	A School Law Retreat (October 1997) Phoenix, Arizona		$160.00	$200.00	
06-154-1	Sharpen Your School Law Focus (January 1996) Aspen, Colorado		$160.00	$200.00	
06-138-1	Practice Forms for School Litigation in Federal Courts (April 1992) — notebook alone		$80.00	$100.00	
	Notebook plus wordprocessing diskette		$150.00	$190.00	
06-125-1	School Law Library Filing System		$12.00	$15.00	

* Member price is extended to NSBA Council of School Attorneys' members and NSBA National Affiliate School Districts.

Subtotal*	
Shipping/Handling Charges	
4.5% Sales tax (Va. Residents)	
TOTAL	

SHIPPING AND HANDLING CHARGES
(to All U.S. Zip-Coded Areas Only)

$ AMOUNT OF ORDER	SURFACE SHIPPING CHARGE
Up to $100.00	$7.00
$100.01 & Above	7% of order Total

Return this form to: NSBA Distribution Center
P.O. Box 161
Annapolis Jct., MD 20701

To order by phone call NSBA at 800/706-6722, or FAX form to 301/604-0158

Publications of the National School Boards Association's ITTE: Education Technology Programs and its Technology Leadership Network

Models of Success: Case Studies of Technology in Schools (*Available Spring 1999*) Softbound. Planning and policy documents are printed alongside the narratives describing what 20 school districts have achieved with technology in this exciting new collection of case studies. Chapters divide the studies according to how education leaders have used technology to support student achievement, technology infrastructure, professional development, and community-wide learning. Featured projects cover a wide range of issues, such as student-managed computer networks, information literacy, acceptable use policies, volunteer support, school/business partnerships, laptop computers, parental involvement, at-risk students, distance learning, and school restructuring. Published with support from Microsoft Corporation, this book concentrates on the choices school leaders make to reach their goals. You'll find models and documents – and contacts – that will help you construct and refine your own success stories. TLN & NA price $28; regular price $35. Order # 03-146-44

Legal Issues & Education Technology: A School Leader's Guide (1999) Softbound, 96 pages. School districts that use new technologies without establishing strong usage policies can incur legal liability and jeopardize the safety and privacy of students, faculty, and staff. This book, written in by leading members of NSBA's Council of School Attorneys, helps you tackle the challenge of striking a healthy balance between protection and open communications. Readers are guided through the top issues – Internet filtering, acceptable use policies for Internet access, copyright and fair use, privacy rights, and freedom of expression – as well as peripheral questions on topics such as open meeting "sunshine" laws for school boards, attorney/client privilege, sexual harassment, Americans with Disabilities Act compliance, and Year 2000 "computer bug" preparedness. Appendices lead readers to Web sites for updated guidance and policy samples. A glossary of technology terms is included. TLN & NA price $28; regular Price $35. Order # 03-145-44

Leader's Guide to Education Technology (1998) Softbound, 24 pages. If you're facing tough technology decisions, turn to this valuable resource that combines research, analysis, and recommendations to help you make sound technology decisions by focusing on student achievement, educational equity, and workforce preparedness. Here you'll find empirical evidence of how technology makes a difference in teaching and learning as well as examples of the challenges that schools face and sample questions to ask when considering technology acquisition and use. This is a guide to hand to others who need to "get on board" the school improvement effort. Published by the EDvancenet project – a partnership of the National School Boards Foundation, the Consortium for School Networking, and MCI WorldCom – it is also available at http://www.edvancenet.org. TLN & NA price $8; regular price $10. Order # 03-144-44

Technology & School Design: Creating Spaces for Learning (1998) Softbound, 124 pages. Whether you're designing new school buildings or remodeling old ones, this essential guide will help you plan for the technology you need, hire skilled architects and technology consultants, work with those professionals to design effective learning spaces, choose the best strategies and equipment, stay within budget, and develop community support and funding. You'll want to consult this book – written by leading school architects and technology consultants – as you develop technology plans, make upgrades to school and district infrastructure, and refine the synergy between people and facilities in your learning environment. TLN & NA price $28; regular price $35. Order #03-143-44

Education Leadership Toolkit: A Desktop Companion (1997) Softbound, 32 pages. This toolkit is a concise introduction to the issues that school board members and other education leaders often face as they integrate technology into their districts' activities and operations. Designed to prompt discussion and exploration, the Desktop Companion is divided into scenarios with questions to consider, followed by tips and resources for developing an approach to the issues raised. The publication offers a user-friendly approach to navigating the wealth of material available in the Education Leadership Toolkit Web site (http://www.nsba.org/sbot/toolkit). TLN & NA price $8; regular price $10. Order # 03-142-44

Investing in School Technology: Strategies to Meet the Funding Challenge / School Leader's Version (1997) Softbound, 80 pages. Providing cost estimates, matrices, and case studies, this book provides how-to help for improving your technology funding practices. NSBA, with support from AT&T Capital Corporation, has developed this *School Leader's Version* based on a report developed by the U.S. Department of Education's Office of Educational Technology and available at the department's Web site. The *School Leader's Version* tailors information specifically to the needs of school leaders and includes a guide to recommended resources on funding, technology, and education reform. TLN & NA price $20; regular price $25. Order # 03-140-44

Technology for Students with Disabilities: A Decision Maker's Resource Guide (1997) Softbound, 100 pages. This valuable guide helps education leaders recognize technology as an essential ally in the effort to aid students who have learning problems, major cognitive disabilities or physical disabilities, and offers strategies for technology implementation to improve curriculum, assessment and administration. Readers will find assistance in evaluating their needs; choosing and funding technology; and creating policy frameworks, long-range technology plans and due process procedures. An extensive resource list (also available on the Web at http://www.nsba.org/itte) provides contact information and describes national, state and local organizations, information centers, clearinghouses and researchers who offer assistance. Published by NSBA and the U.S. Department of Education's Office of Special Education Programs. NSBA Technology Leadership Network and National Affiliate district price $20; Regular Price $25. Order # 03-138-44

Leadership & Technology: What School Board Members Need to Know (1995) Softbound, 194 pages. School districts need an informed school board to help technology plans move forward. Topic by topic, issue by issue, this book grounds board members in the knowledge they need to ask the right questions and initiate appropriate policies regarding technology use in schools. In an easy-to-read, discussion guide format, it helps the board — and administrators — hurdle the barriers to change, understand the importance of their leadership, prepare for technology planning, and confront important technology-related issues such as purchasing, staff development, curriculum revision, facility improvement, and evaluation. An extensive glossary and bibliography further support readers along the learning curve. TLN & NA price $28; regular price $35. Order # 03-135-44

Plans & Policies for Technology in Education: A Compendium (1995) Softbound, 250 pages. Presenting a wide collection of numerous school districts' actual technology plans and policies, this is a reference work and guide that school leaders have long needed. Divided by plans/policies and then by topic — such as purchasing, copyright, network/Internet use, ethics, staff development, curricular integration, technology access, equity, community involvement, evaluation, and more — the appropriate portions of 35 districts' formatted documents appear as samples to consider when creating and revising your own plans and policies. In separate sections, the book also guides administrators and board members through the steps of planning and policy-setting, provides tips and warns of traps, reprints full technology plans, offers sample job descriptions and survey guides, and recommends additional resources. TLN & NA price $28; regular price $35. Order # 03-133-44

Electronic School (Quarterly magazine, approx. 40 pages) Designed as a helpful resource for all school personnel, *Electronic School* colorfully covers school technology trends and presents case studies that reveal strategies of K-12 schools nationwide. Feature articles look in-depth at topics such as staff development, funding, telecommunications, and school restructuring. Published by NSBA's magazine, *The American School Board Journal*, *Electronic School* is mailed to 12 designated contacts in each NSBA Technology Leadership Network school district as a benefit of membership. To receive *Electronic School* as a quarterly supplement *to The American School Board Journal*, dial (703) 838-6721. Per issue: TLN & NA price $4; regular price $5. Order # 03-101-44

Telecommunications and Education: Surfing and the Art of Change (1994) Softbound, 124 pages. This easy-to-read guide helps telecommunications novices consider the benefits and learn the basics of going online using computer, telephone, and modem. The authors, education technology consultants, recommend that educators first use smaller telecommunications networks before they venture onto the worldwide Internet "network of networks." Contact information is provided both for Internet and other network access providers. A glossary, resources, sample policies for Internet use, and a needs assessment chart are included. TLN & NA price $28; regular price $35. Order # 03-131-44

Multimedia and Learning: A School Leader's Guide (1994) Softbound, 116 pages. This is a comprehensive guide for school leaders seeking to implement multimedia. It includes descriptions of multimedia technologies and trends; research-based studies and theories of multimedia environments; actual case studies of multimedia in schools; multimedia applications for education; facilities planning, staff development, and copyright issues; a glossary; and recommended information sources. TLN & NA price $28; regular price $35. Order # 03-129-44

Teachers and Technology: Staff Development for Tomorrow's Schools (1991) Softbound, 184 pages. School leaders who help teachers learn to apply technology will find methods, philosophies, research, resource lists, and case studies in this guide. Planning, peer training, Constructivist training, internship opportunities, and distance learning are among the topics discussed. TLN & NA price $28; regular price $35. Order # 03-107-44

Technology Leadership News, the newsletter of NSBA's ITTE, is filled with information on new issues, trends, products, programs, technology applications, district profiles, case studies, government initiatives, funding, video conferences, and other opportunities and news of interest. Written in layman's terms and published nine times annually, it is mailed to 12 individuals in each NSBA Technology Leadership Network school district as a benefit of TLN participation. TLN participants also receive full-staff copying/distribution rights. Others may purchase annual subscriptions for $75. Order # 03-119-44

See publications' Tables of Contents on the Internet's World Wide Web at http://www.nsba.org/itte/publicat.html **and order using form on next page.**

Order Form for Publications of National School Boards Association's ITTE: Education Technology Programs and its Technology Leadership Network

To order please complete this order form
and return it by mail to NSBA Distribution Center, P.O. Box 161, Annapolis Jct., MD 20701-0161.
To order by phone, call NSBA at 800-706-6722. To order by FAX, dial NSBA at 301-604-0158.

SHIP TO: (Street address—all orders sent UPS)

Name _____

Title _____

Organization _____

Street Address _____

City _____ State _____ Zip _____

Phone (_____) _____

BILL TO: (if other than ship to)

Name _____

Title _____

Organization _____

Street Address _____

City _____ State _____ Zip _____

Phone (_____) _____

Title	Quantity	Discount Price*	Regular Price	Total
Models of Success: Case Studies of Technology in Schools 03-146-44		$28.00	$35.00	
Legal Issues & Education Technology: A School Leader's Guide 03-145-44		$28.00	$35.00	
Leader's Guide to Education Technology 03-144-44		$8.00	$10.00	
Technology & School Design: Creating Spaces for Learning 03-143-44		$28.00	$35.00	
Education Leadership Toolkit: A Desktop Companion 03-142-44		$8.00	$10.00	
Investing in School Technology: Strategies to Meet the Funding Challenge 03-140-44		$20.00	$25.00	
Technology for Students with Disabilities: A Decision Maker's Resource Guide 03-138-44		$20.00	$25.00	
Leadership & Technology: What School Board Members Need to Know 03-135-44		$28.00	$35.00	
Plans & Policies for Technology in Education: A Compendium 03-133-44		$28.00	$35.00	
Electronic School 03-101-44 (To receive latest issue)		$4.00	$5.00	
Telecommunications and Education: Surfing and the Art of Change 03-131-44		$28.00	$35.00	
Multimedia and Learning: A School Leader's Guide 03-129-44		$28.00	$35.00	
Teachers and Technology: Staff Development for Tomorrow's Schools 03-107-44		$28.00	$35.00	
Technology Leadership News (9 issues annually) 03-119-44		TLN Benefit	$75.00	
			SUBTOTAL:	
			SHIPPING AND HANDLING: (see charges below)	
			TOTAL:	

❒ My check made payable to NSBA in the amount of $ _____ is enclosed.

❒ Bill me using P.O. # _____ ($20 minimum order)

Please charge my: ❒ VISA ❒ MasterCard ❒ American Express

Card Number

Expiration Date

Name (please print)

Authorized Signature

For more information about the content of NSBA's technology publications or about the Technology Leadership Network, contact Anne Ward at NSBA, 1680 Duke St., Alexandria, VA 22314, (703) 838-6214, e-mail: award@nsba.org. For information about NSBA's National Affiliate Program, contact Bonita Metz at that address, (703) 838-6746, e-mail: bmetz@nsba.org.

* These publications are discounted to NSBA National Affiliate and Technology Leadership Network districts.
To receive this discount you must check one of the spaces below:

❒ My district is a National Affiliate, # _____

❒ My district participates in the Technology Leadership Network.

Shipping and Handling Charges
(to all US Zip-Coded Areas only)

$ Amount of Order	**Surface Shipping Charge**
up to $100.00	$7.00
$100.01 - and above	7% of total order

Shipping and handling charges for Canadian/overseas orders will be billed at $7.00 plus actual postage. Quantity discounts available: for information call 800-706-6722.

Visit us on the Web!
See Tables of Contents and more at
http://www.nsba.org/itte/publicat.html

About the NSBA Council of School Attorneys . . . .

Leadership in legal advocacy for public schools has been the overriding mission of the NSBA Council of School Attorneys throughout its celebrated history. Almost 3,000 members strong today, the Council was formed in 1967 to provide information and practical assistance to attorneys who represent public school districts. It is the only national advocacy organization composed exclusively of attorneys representing school boards. It offers continuing legal education, specialized publications, a forum for exchange of information, and it supports the legal advocacy efforts of the National School Boards Association. For information on membership, contact your state school boards association or the NSBA Council of School Attorneys.

The Council accepts individual attorney members and has an affiliate member agreement with the following state attorneys' councils: Alabama, Arizona, Arkansas, California, Colorado, Delaware, Florida, Georgia, Illinois, Iowa, Kansas, Louisiana, Maine, Maryland, Massachusetts, Michigan, Mississippi, Missouri, Montana, Nebraska, New Hampshire, New Jersey, New Mexico, New York, North Carolina, North Dakota, Oklahoma, Oregon, Pennsylvania, South Carolina, South Dakota, Tennessee, Texas, Vermont, Virginia, and West Virginia.

Web site: http://www.nsba.org/cosa

About the NSBA ITTE: Education Technology Programs

The National School Boards Association established the ITTE: Education Technology Programs (formally known as the Institute for the Transfer of Technology to Education) in 1985 to advance the wise and appropriate use of technology in public education. The Technology Leadership Network, a major component of ITTE, was created in 1986 to help school districts share in dialogue about technology in education.

Special reports such as this one are among the benefits of participation in the Technology Leadership Network. *Technology Leadership News* newsletter, the annual Technology + Learning Conference, site visits to exemplary school districts, topical meetings, and an online list serve are some of the additional opportunities.

See ITTE's Web site, http://www.nsba.org/itte, for information on events, activities, publications, and the 460 school districts currently participating in the Technology Leadership Network, or contact the ITTE staff at NSBA, 1680 Duke St., Alexandria, VA 22314, (703) 838-6722.

about NSBA...

The National School Boards Association is the nationwide advocacy organization for public school governance. NSBA's mission is to foster excellence and equity in public elementary and secondary education in the United States through local school board leadership. NSBA achieves its mission by amplifying the influence of school boards across the country in all public forums relevant to federal and national education issues, by representing the school board perspective before federal government agencies and with national organizations that affect education, and by providing vital information and services to Federation Members and school boards throughout the nation.

NSBA advocates local school boards as the ultimate expression of the unique American institution of representative governance of public school districts. NSBA supports the capacity of each school board—acting on behalf of and in close concert with the people of its community—to envision the future of education in its community, to establish a structure and environment that allow all students to reach their maximum potential, to provide accountability for the people of its community on performance in the schools, and to serve as the key community advocate for children and youth and their public schools.

Founded in 1940, NSBA is a not-for-profit federation of state associations of school boards across the United States and the school boards of the District of Columbia, Guam, Hawaii, and the U. S. Virgin Islands. NSBA represents the nation's 95,000 school board members. These board members govern 14,772 local school districts that serve more than 46.5 million public school students—approximately 90 percent of all elementary and secondary school students in the nation. Virtually all school board members are elected; the remainder are appointed by elected officials.

NSBA policy is determined by a 150-member Delegate Assembly of local school board members from throughout the nation. The 24-member Board of Directors translates this policy into action. Programs and services are administered by the NSBA executive director, assisted by a professional staff. NSBA is located in metropolitan Washington, D.C.

NSBA's Programs and Services

- **National Affiliate Program** — enables school boards to work with their state association and NSBA to identify and influence federal and national trends and issues affecting public school governance.
- **Council of Urban Boards of Education** — serves the governance needs of urban school boards.
- **Large District Forum** — serves the governance needs of large but non-urban boards.
- **Rural and Small District Forum** — serves the governance needs of rural and small enrollment districts.
- **Federal Relations Network** — school board members from each congressional district actively participate in NSBA's federal and national advocacy efforts.
- **Federal Policy Coordinators Network** — focuses on the administration of federally funded programs.
- **Award Winning Publications — *The American School Board Journal*, *School Board News***, and special substantive reports on public school governance throughout the year.
- **Institute for the Transfer of Technology to Education and Technology Leadership Network** — advance public education through best uses of technology in the classroom and school district operations.
- **Council of School Attorneys** — focuses on school law issues and services to school board attorneys.
- **Annual Conference and Exposition**--the nation's largest policy and training conference for local education officials on national and federal issues affecting the public schools in the United States.
- **National Education Policy Network** — provides the latest policy information nationwide and a framework for public governance through written policies.
- **Training/Development and Resource Exchange** — for the policy leadership of state school boards associations and local school boards.

National School Boards Association
1680 Duke Street
Alexandria, VA 22314-3493
Phone: 703-838-6722
Fax: 703-683-7590

Web Address: http://www.nsba.org *E-Mail: info@nsba.org*

Excellence and Equity in Public Education through School Board Leadership

NATIONAL SCHOOL BOARDS ASSOCIATION
1680 DUKE STREET
ALEXANDRIA, VIRGINIA 22314-3493
PHONE: 703-838-6722
FAX: 703-683-7590

WEB ADDRESS: www.nsba.org
E-MAIL: info@nsba.org

EXCELLENCE AND EQUITY IN PUBLIC EDUCATION
THROUGH SCHOOL BOARD LEADERSHIP